الجزء الأول

الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة

وزارة التّعليم العاليّ والبحث العلميّ

جامعة مولود معمري، تيزي-وزو

كلّيّة الآداب واللّغات /قسم اللّغة العربيّة وآدابها

مخبر الممارسات اللغوية في الجزائر

الملتقى الوطنيّ حول:

الأمن المعلوماتيّ: مُهدّداته وسُبُل الحماية

03-04 نوفمبر 2015



المُسهِمون في إنجاز الملتقى:

- جامعة تيزي-وزو؛
- مخبر الممارسات اللّغويّة في الجزائر؛
- سلطة الضّبط للبريد والمواصلات السّلكيّة واللاّسلكيّة (ARPT)؛
- الشّركة الوطنيّة لتوزيع الكهرباء والغاز (SONELGAZ).

اللّجنة العلميّة:

- أ. د. صالح بلعيد، مدير المختبر؛
- د. نصيرة إدير، رئيسة اللّجنة العلميّة؛
- أ. ياسين بوراس، عضوا؛
- أ. كاهنة محيوت، عضوة؛
- أ. أحلام بن عمرة، عضوة؛
- أ. كاهنة لرول، عضوة.

ردمك: 978 -9961 -9786 -9- 6



منشورات مختبر الممارسات اللغوية في الجزائر
2016



الفهرس



برنامج الملتقى

الجلسة الافتتاحيّة: 09.00 سا
كلمة رئيـــسة اللَّجنة العلميّة
كلمة ترحيبيّة لمدير مخبر الممارسات اللّغويّة
كلمة رئيس قسم اللغّة العربيّة وآدابها
كلمة عميدة كلّيّة الآداب واللّغات
افتتاحيّة رئيس الجامعة
تكريمات
استـــراحة

برنامج الجلسات العلميّة

اليوم الأوّل: 03-11-2015 الفترة الصَّباحيّة:

رئيس الجلسة الأولى: د. الصّدّيق بسّو			
التّوقيت	الأستاذ (ة)	عنوان المحاضرة	الجامعة
11:00-11:15	د. الصّدّيق بسّو	البرامج مفتوحة المصدر والأمن المعلوماتيّ	ج/ سطيف
11:15-11:30	د. حسنية عزاز	الأمن اللّغوي منطلق للأمن المعلوماتيّ -مهدّداته ومستلزماته-	ج/ سيدي بلعباس

11:45-11:30	د. زهرة بوخاتمي	نظام الموزّع الإلكترونيّ في المؤسّسات التّعليميّة	ج/ سيدي بلعباس
12:00-11:45	د. فاطمة صغير	دَورُ الأمن المعلوماتيّ في حِماية البحوث والدّراسَاتِ العِلميّة	ج/ تلمسان
12:15-12:00	أ.د. فهد سالم خليل الرّاشد	إدارة مكتبة معهد الخرطوم الدّوليّ للّغة العربيّة مشروع إدارة مكتبة رقميّة معلوماتيّة آمنة	باحث لغويّ الكويت
13:00-12:15	مناقشة عامّة		

اليوم الأوّل: 03-11-2015 الفترة المسائيّة:

رئيس الجلسة الثّانية: أ.د. فهد سالم خليل الرّاشد			
التّوقيت	**الأستاذ (ة)**	**عنوان المحاضرة**	**الجامعة**
14:15-14:00	أ. مليكة بوخاري	مهدّدات الهويّة الجزائريّة والجرائم الالكترونيّة بين التّشريع والتّطبيق	المدرسة الوطنيّة العليا لعلوم الإعلام والصّحافة
14:30-14:15	د. محمّد يونسي	واقع الملكيّة الفكريّة في عصر التّسارع الرّقمي	ج/ تيسمسيلت

14:45-14:30	د. الصدّيق حاجيّ	السّرقات الإلكترونيّة، تجلّياتها وانعكاساتها على البحث العلميّ وسبل الحدّ من مخاطرها	ج/ قسنطينة
15:00-14:45	أ. نزهة خلفاوي أ. سعاد عبّاسي	الرّسائل العلميّة الجامعيّة في المكتبات الرّقمية بين النّفاذ الحرّ للمعلومات وسرقات الملكيّة الفكريّة	وحدة البحث واقع اللّسانيات وتطوير الدّراسات اللّغويّة في البلدان العربيّة – تلمسان-
15:15-15:00	أ. شيماء درّاجي	مفهوم الأمن المعلوماتيّ وواقع الجريمة الإلكترونيّة في مذّكرات طلبة السّنة الثّالثة ليسانس ل.م.د قسم اللّغة العربيّة وآدابها -جامعة منتوري قسنطينة أنموذجا-	ج/ قسنطينة
16:00-15:15	مناقشة عامّة		

اليوم الثّاني: 04-11-2015 الفترة الصّباحيّة:

رئيس الجلسة الثّالثة: د. الصّديق حاجّي			
التّوقيت	الأستاذ(ة)	عنوان المحاضرة	الجامعة
09:15-09:00	أ. كاهنة شاطري	العلاقة التّأثيريّة بين الأمن المعلوماتيّ والأمن القوميّ للدّول: بين متطلّبات التّطور والتّكامل ورهانات التّهديدات	ج/ تيزي-وزو
09:30-09:15	أ. ياسين بوراس	تقنيات التّعايش الإلكترونيّ مع الفيروسات لتأمين الملفّات الإلكترونيّة	ج/ تيزي-وزو
09:45-09:30	د. نجيبة بادي بوقميجة	الإطار القانوني لأمن المعلومات	ج/ الجزائر1
10:00-09:45	د. كريمة تدريست	إشكاليّة القانون الواجب التّطبيق على النّزاعات الإلكترونيّة	ج/ تيزي-وزو
10:15-10:00	أ. كاهنة محيوت	الطّبيعة القانونيّة للجريمة الإلكترونيّة وسبل الحدّ منها	ج/ تيزي-وزو
10:45-10:15	مناقشة عامّة		
11:00-10:45	استراحة		

اليوم الثّاني: 04-11-2015 الفترة الصّباحيّة:

رئيسة الجلسة الرّابعة: د. نصيرة إدير			
التّوقيت	الأستاذ (ة)	عنوان المحاضرة	الجامعة
11:00-11:15	د. علجيّة أوطالب	Internet et vie privée	ج/ تيزي-وزو
11:15-11:30	أ. عمر زايدي	Techniques de la Reconnaissance Automatique de la Parole, Application pour la langue arabe	ج/ باتنة
11:30-11:45	أ. حجيلة قلاّز	Les ressources de protection contre les menaces de la sécurité des systèmes d'information	ج/ تيزي-وزو
11:45-12:00	أ. ليلى يمينة موساوي	دراسة تقابليّة إنجليزيّة/عربيّة لمصطلحات عالم الاختراق وعلاقتها بالأمن المعلوماتي	وحدة البحث واقع اللّسانيات وتطوير الدّراسات اللّغويّة في البلدان العربيّة – تلمسان-
12:00-12:15	أ. زينب لمونس	انطلاقة شبكات الحاسبات الإلكترونيّة العالميّة	ج/ قسنطينة
12:15-13:00	مناقشة عامّة		

اليوم الثّاني: 04-12-2015 الفترة المسائيّة:

رئيسة الجلسة الخامسة: د. الجوهر مودر			
التّوقيت	الأستاذ (ة)	عنوان المحاضرة	الجامعة
14:15-14:00	أ. محمّد الهادي عايش	معزّزات الجريمة الإلكترونيّة وواقع الأمن المعلوماتيّ دراسة ميدانيّة لعيّنة من تقنيّي الحماية وبعض محترفي الاختراق	ج/ قسنطينة
14:30-14:15	أ. عبد الحفيظ شريف	حقّ حيازة الفكرة العلميّة وأفق شيوع المعرفة بين الالتزامات الأخلاقيّة والمطالبات القانونيّة	ج/ برج- بوعريريج
14:45-14:30	أ.ورديّة قلاّز	الأخطار والمشاكل المعاصرة الّتي تواجهها الأنظمة المعلوماتيّة (الفيروسات، وقرصنة المعلومات).	ج/ تيزي-وزّو
15:00-14:45	أ. أحلام بن عمرة	جهود المنظّمة العالميّة للتّقييس الأيزو (ISO) في تحقيق الأمن المعلوماتيّ	ج/ تيزي-وزّو
15:30-15:00	مناقشة عامّة		

الورشة الأولى: اليوم الأوّل: 03-11-2015

عنوان الورشة: مدخل إلى مفهوم الأمن المعلوماتيّ رئيس الورشة: أ. عبد الحفيظ شريف 14:00-16:30 سا، القاعة السّفلى بالمسمّع		
أعضاء الورشة		
الأستاذ (ة)	عنوان المحاضرة	الجامعة
أ. كمال رمضاني	الأرشيف بين التّوثيق والأمن المعلوماتيّ	ج/ الشّلف
أ. خديجة حامي	الأنظمة المعلوماتيّة في مواجهة القرصنة والتّخريب (المخاطر المحدّقة والحلول النّاجعة)	ج/ تيزي-وزّو
أ. فاتح مرزوق	دور الموسوعات العلميّة في كشف السّرقات الشّعريّة	ج/ تيزي-وزّو
أ. رادية حجبار	القراءة من ملف نصيّ في لغة البرمجة جافا (java)	ج/ تيزي-وزو
أ. كاهنة لرول	تحديد بعض مصطلحات الأمن المعلوماتيّ	ج/ تيزي-وزّو
أ. يحّي فطمة	الهندسة الاجتماعيّة والجريمة الإلكترونيّة	ج/ تيزي-وزو
أ. الشّافعي مالكيّه	تكنولوجيا المعلومات الحديثة وأثارها في تسريب أسئلة الامتحانات تسريب أسئلة الباكالوريا والتّعليم المتوسّط بالجزائر 2015	ج/ خنشلة
أ. حاكم عماريّة	مبرّرات تعزيز صناعة المحتوى الرّقميّ العربيّ	ج/ سعيدة
أ. عبد القادر معبد	الشّابكة والأمن المعلوماتيّ	ج/ تيزي-وزو
	مناقشة عامّة	

الورشة الثّانية: اليوم الثّاني: 04-11-2015

عنوان الورشة: الملكيّة الفكريّة بين الجريمة الإلكترونيّة والقوانين الرّدعيّة رئيس الورشة: أ. فاتح مرزوق 09:00-12:00سا، القاعة السّفلى بالمسمّع		
أعضاء الورشة		
الأستاذ (ة)	**عنوان المحاضرة**	**الجامعة**
أ. سميرة محمّدي	الحماية القانونيّة لحقوق المؤلِّف في ظلّ البيئة الرّقميّة في القانون الجزائريّ	ج/ تيزي–وزو
أ. صليحة شتّيح	إشكاليّة غياب الملكيّة الفكريّة في ظلّ السّرقات الإلكترونيّة	ج/ تيزي–وزو
أ. جميلة علّوشن	الملكيّة الفكريّة بين الحماية والاحتكار	ج/ تيزي–وزو
أ. رضية بركايل	التّنظيم القانونيّ الجزائيّ للجريمة المعلوماتيّة في التّشريع الجزائريّ	ج/ تيزي–وزو
أ. فضيلة لغيمة	الجريمة المرتكبة عبر الإنترنيت والسّبل التّشريعيّة للحدّ منها	ج/ تيزي–وزو
أ. سميّة كرميش	السّرقةُ العلميَّةُ عبرَ الإنتَرنيتْ وحِمايةُ حقُوق الملكيّةِ الفِكريَّة	ج/ قسنطينة
أ. طاوس خلوات	الجرائم الإلكترونيّة: نظام مكافحتها والمعوّقات المقلّلة من استخدام التّقنيّة الحديثة	ج/ تيزي–وزو
أ. فطيمة ذيب	ضرورة مكافحة جرائم الحاسبات الإلكترونيّة	ج/ قسنطينة
أ. تهامي بلعقون	دور اللّسانيات الحاسوبيّة في تحقيق الأمن المعلوماتيّ	ج/ تيزي وزو
أ. مولود بوزيد	الأمن المعلوماتيّ ومهدّداته، الشّبكة الاجتماعيّة	ج/ تيزي–وزو

	-الفيسبوك- أنموذجا	
مناقشة عامّة		

لجنة اقتراح مشروع الملتقى القادم:
1- أ.د. فهد خليل سالم الرّاشد 2- د. الجوهر مودر 3- د. حياة خليفاتي 4- د. نصيرة إيدير

الجلسة الختاميّة:
رئيس الجلسة الختاميّة: أ.د. صالح بلعيد
- قراءة تقرير الورشة الأولى؛ - قراءة تقرير الورشة الثّانيّة؛ - قراءة مشروع الملتقى القادم؛ - كلمة ختاميّة لمدير المختبر.



كلمة رئيسة اللَّجنة العلمية

د. نصيرة إدير

بسم الله الرحمن الرحيم

والصلاة والسلام على أشرف المرسلين

- السيد رئيس الجامعة؛
- السيدة عميدة كليّة الآداب واللّغات؛
- السادة نوّاب عميدة الكلية؛
- السيد رئيس قسم اللُّغة العربية وآدابها؛
- السيد مدير مخبر الممارسات اللّغوية في الجزائر؛
- السيدات والسادة الأساتذة الأفاضل، ضيوفا ومحليين؛
- أيَّتُها الطالبات؛ أيُّها الطلبة؛
- السيدات والسادة الحضور؛ السّلام عليكم ورحمة الله تعالى وبركاته وطاب صباحكم.

مرة أخرى، تفي جامعة مولود معمري بتيزي–وزو ممثَّلة في مخبر الممارسات اللّغوية في الجزائر بوعدها، وتقف عند الموعد الذي ضربته لنا منذ ما يقارب العامّ، لتجمعنا اليوم في ملتقاها الوطني الموسوم بـــ **(الأمن المعلوماتيّ: مُهدّداته وسبل الحماية).** هذا الموضوع الذي أضحى من ضرورات البحث العلميّ في عصرنا الحاليّ، وبخاصة مع دخول تقنيّات الإعلام والاتّصال الحديثة إلى مجتمعاتنا، فبالقدر الذي أسهمت به في الرّقيّ والتّطوّر وتقريب المسافات بين الشّعوب، نجدها أفرزت الكثير من السّلبيّات، لعلّ أهمّها: صعوبة احتفاظ الفرد بخصوصيّاته، وانتهاك الملكيّة الفكريّة، وخرق المبادئ والأخلاق، وتهميش الهويّة. وفي ظلّ هذا الواقع، أصبحت ثمّة حاجة ماسّة للتّعرّف على هذه الانتهاكات والتّوعية بها، ومتابعتها، وسنّ القوانين والتّشريعات اللاّزمة لمكافحتها.

وتكمن أهمية هكذا موضوع في علاج ظاهرة عصريّة، تخصّ شبكة المعلومات التي صارت تُعتمد في كلّ الميادين، العلميّة، والإداريّة، والعسكريّة والاقتصاديّة... إلخ، وتنذر بتحديات جمّة، تؤدي أحيانا إلى سحب الثقة من الأفراد العلميين والمؤسّسات، وإلى تهديد أمن بيئة الاتصالات عبر الشّبكة؛ حيث تتعرّض هذه الشبكة إلى خروق عديدة، وإلى اعتداءات رقميّة، وهجمات فيروسيّة، وتُعتَمَد في قرصنة أفكار الغير وتبنّيها، أو ما يُسمَّى السَّطو على الملكية الفكريّة.

من هذا المنطلق، ووعيا بهذه الحقيقة اليوم، ارتأى مخبر الممارسات اللّغوية في الجزائر، في إطار انفتاحه على الفروع المعرفيّة المعاصرة، برئاسة الأستاذ الدكتور صالح بلعيد، عقد ملتقاه الوطني في موضوع **الأمن المعلوماتيّ: مهدداته وسبل الحماية** سعيا منه إلى التعريف به واستنهاض هِمَم الباحثين للحدّ من مهدداته ومشاكله، والتوصّل إلى خطة علميّة لإيجاد البدائل النّوعية التي من شأنها الحماية منها. فأبى إلاّ أن يخطّط لهذا الملتقى بتحديد إشكالاته، ورسم محاوره المختلفة وتسطير أهدافه، ودعا لذلك الأساتذة والباحثين والمتخصّصين من جامعات الوطن؛ للإسهام في إثراء الموضوع بالنّقاش والحوار، وعرض أهمّ ما توصلت إليه أبحاثهم، ومعاينة المقاربات التّنظيرية والنّماذج التطبيقية التي كلّلت بالنّجاح فاستجاب لهذه الدعوة عدد كبير من الباحثين والباحثات من الأساتذة والطلاب من كلّ ربوع الوطن، إذ بلغ عدد المداخلات المقترحة ستين (60) مداخلة، قبلت منها ثلاث وأربعون (43) مداخلة بعد عملية التّحكيم التي باشرتها اللّجنة العلميّة للملتقى مشكورة.

وتنتظم هذه المداخلات في ثمانية (08) محاور، ويوزّع عرضها حسب البرنامج الذي بين أيديكم، في خمس (05) جلسات عامة، وورشتي عمل (02) تحمل الورشة الأولى عنوان "**مدخل إلى مفهوم الأمن المعلوماتي**"، وتحمل الورشة الثانية عنوان "**الملكية الفكرية بين الجريمة الإلكترونية والقوانين الردعية**". وقد

خصّصت لهما على التّرتيب أمسية اليوم الأوّل، وصبيحة اليوم الثّاني، بإحدى القاعات التابعة للمسمّع. وهو ما سيشهده منتداكم على مدار يومين كاملين.

ولا يفوتني في هذا المقام، أن أعرب عن خالص تقديري وامتناني للأستاذ الدكتور صالح بلعيد على الثقة التي أولاني إياها، والشرف الذي خصّني به مرة ثانية لتولي رئاسة الملتقى، وأن أتوجّه بالشّكر والعرفان إلى أعضائها، وما كان لهذا الإنجاز أن يتحقّق لولا جهودهم المبذولة.

كما أنوّه بكرم الإسهام المادي لسلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية للمرة الثانية على التوالي، فنرجو لممثليها إقامة طيبة بيننا، وكذا الشركة الوطنية لتوزيع الكهرباء والغاز (سونلغاز) التي التحقت بها هذه السنة، وهذا الإسهام معنوي أكثر منه مادي يندرج في إطار خدمة الشأن العام، وأَكرِمْ بهم من رجال يخدمون الشأن العام.

وقبل الختام، إليكم ملخصا لموضوع الملتقى وإشكاليته باللغة الإنجليزية:

Communication in modern society is undergoing rapid changes prompted by the recent technological advances in the computer and telecommunication industries. Computer systems and networks have been specifically the target of an uncountable electronic scams and violations. Therefore **Information Security** has now become a major preoccupation for the international community.

Personal data and strategic information in all forms need constantly to be protected from being spied and abused by individuals or organizations for whom it was not intended. This will help develop a coherent strategy for the insurance of privacy and intellectual property against cyber-crime and the loss of trust and ethical values that can cause enormous damages going deep into all the aspects of life, especially peace and internal security.

The Arab world has not been sheltered from this risk. It’s highly vulnerable to the insecurity of information, as it relies on importing technology and is a weak partner in the world market.

In this context, The Laboratory of Language Practices in Algeria has taken the initiative to organize this National Conference about

“**Digital Information Security: Risks and protection measures”.** It intends to bring together professional, scholars and researchers and to facilitate exchanges between them in order to shed light on how the world is dealing with Information Security issues; to assess the impact that would be on both individuals and organizations; and to review ways in which digital information can be secured and protected against threats in a borderless world.

وإليكم الآن ملخصا باللغة الفرنسية:

La communication dans la société moderne revêt une importance grandiose et connaît des changements rapides dus aux récentes avancées technologiques dans les industries de l'informatique et des télécommunications. Les systèmes et réseaux d’informations ont été spécifiquement la cible d’innombrables escroqueries et violations électroniques. Ainsi, la sécurité de l'information internationale est devenue une préoccupation majeure pour la communauté.

Toutes les données à caractère personnel et stratégique ont constamment besoin d'être protégées contre toutes formes d’espionnage et d’abus par des individus ou organisations non autorisés à y accéder. La mise en place d’une stratégie cohérente devient alors une condition *sine qua non* pour assurer la protection de la vie privée et de la propriété intellectuelle contre la cybercriminalité et la perte de confiance et de valeurs éthiques, qui peuvent causer des dommages énormes affectant profondément tous les aspects de la vie, notamment la paix et la sécurité intérieure.

Le monde arabe n'est pas à l’abri de ce risque, et se trouve très vulnérable à l'insécurité de l'information, de par sa position de partenaire faible, et de par son statut de grand importateur de technologie sur le marché mondial.

Dans ce contexte, le Laboratoire des Pratiques Langagières en Algérie dédie son colloque national au thème de **"La Sécurité de l'Information Numérique: Risques et Mesures de Protection**".

Il se veut être un forum de réflexion, de débat et de discussion où se côtoient chercheurs, universitaires et professionnels. Il vise à faciliter les échanges entre eux, et à faire le point sur la façon dont la question de la sécurité de l'information numérique est approchées tant

au niveau national qu'international; à en évaluer l'impact éventuel sur les individus et sur les institutions, et à étudier les voies et moyens de protection contre les risques qui la guettent dans un monde sans frontières.

وفي الختام، وباسم أعضاء اللّجنة العلميّة للملتقى، أتوجّه بالشّكر الجزيل إليكم أنتم الذين لبيتم دعوتنا، من جامعة تيزي- وزو ومن جامعات الوطن المختلفة ومخابرها، فتحملتم وُعْثاء السفر لتقدموا أبحاثكم دعما لمسيرة التميّز والعطاء أسأل الله تعالى أن يجزل لكم العطاء على ما بذلتموه، وآمل أن تجدوا في ملتقانا التحدي العلمي فترفعوه، كما يسعدني أن أرحب بكم بيننا مجددا وأتمنى لكم مقاما طيبا كريما، ودمتم في خدمة البحث والعلم.

والسّلام عليكم.

إشكالية الملتقى

تتأسّس إشكاليّةُ الملتقى على مجموعة تساؤلات تتراكب لتحدّد سؤالا جوهريّا هو:

ما هي المخاطر التي تتهدد أمن المعلومات مع دخول تقنيّات الإعلام والاتّصال الحديثة إلى مجتمعاتنا ؟ وما سبل الحماية منها؟

وتتفرع عنها مجموعة الإشكالات التّالية:

- ما موقعنا –نحن العرب– الذين لا نحتكم إلى آليات التّحصين والأمن وبخاصة ونحن نتوجه نحو العمل بالحكومات الإلكترونيّة، في المعاملات الإداريّة والاتّصالات الاجتماعيّة، والأبحاث العلميّة؟
- ما حيلتنا في حال تعرّضت هذه الشّبكة للتّخريب؟
- كيف يكون تعاملنا الشّبكي مع الشّريك الأجنبي المتفوّق في استعمال التِّقانة؟
- هل أعددنا قواعد الاحتياط لما قد يحصل من قرصنة؟
- ما العمل بعد وصول الغوّاصين في الشّابكة إلى كلمة السر؟
- كيف يتمّ الحدّ من ظاهرة الاعتداء على الملكيّة الفكريّة للغير؟
- أليس هنا يكمن الخطر كلّ الخطر؟

كلمة مدير المخبر

بسم الله الرحمن الرحيم، وبعد؛

باسمي الشخصي، وباسم أعضاء مخبر الممارسات اللّغوية في الجزائر، ومقرّه جامعة مولود معمري بتيزي–وزو، وباسم اللّجنة العلمية للملتقى الوطني الموسوم: الأمن المعلوماتي: مُهدِّداتــه وسُبــل الحمايــة، نرحّــب بكم جميعاً، ونرفع للشعب الجزائري آيات التقــدير والتهــاني بمناسبة الذكرى الواحدة والستين لاندلاع الثــورة التحريريــة التــي لولاهــا مــا كنّا هنا، ولولا تلك الفئات الشهيدة والمجاهدة لبقينا سفلة حقيرين تحت نير الكولون، فأنعم بأولئك الذين قال الله فيهم: ﴿ مِّنَ ٱلْمُؤْمِنِينَ رِجَالٌ صَدَقُواْ مَا عَٰهَدُواْ ٱللَّهَ عَلَيْهِ ۖ فَمِنْهُم مَّن قَضَىٰ نَحْبَهُۥ وَمِنْهُم مَّن يَنتَظِرُ ۖ وَمَا بَدَّلُواْ تَبْدِيلًا ﴿٢٣﴾ ﴾ الأحزاب 23.

زملائي زميلاتي أيّتها الطالبات والطلبة، ومن خلال هذا الفعل العلمي، أسجّل كلّ التقدير لكلّ من أسهم في إنجاز هذا الملتقى، وأخصّ:

ـــ السيد رئيس الجامعة الذي نتمنى له النّجاح في مهمّة التسيير؛

ـــ السادة نواب رئيس الجامعة؛

ـــ السيدة عميدة كلية الآداب واللّغات، وما فتئت تعمل على التّغيير، وتحديث الكلية لما هو أفضل؛

ـــ الزميلات والزملاء ومديرات المخابر؛

ـــ الذين يُحضّرون لنا أسباب النجاح في الجامعة، من إداريين ومصالح مالية ومسؤولي هذا المُسمّع؛

ـــ الذين أسهموا معنا مادياً ومعنوياً، وهم:

- سُلطة الضبط للبريد وتكنولوجيا الاتّصال؛
- شركة سونلغاز؛
- اللّجنة العلمية للملتقى، وعلى رأسهم الفُضلى المتألقة: نصيرة إيدير؛ التي تتفانى في خدمة الشأن العامّ، بما في فريقها من أعضاء يُخلِصون في كلّ أعمالهم؛

ـ الزميلات والزملاء الذين وفدوا إلينا من مختلف الجامعات الوطنية، ومن مراكز البحوث ونتمنى أن يَرضَوْا عنّا، ويعذروننا إذا حدث تقصير، وكلّ نقيصة هي رُغم إرادتنا، ولا في نيّتنا.

ـ الذين لا تنام عيونهم، فهم يسهرون من أجل أن تبقى الجزائر واقفة، فلهم منّا التقدير، ونقول لهم: مزيداً من اليقظة؛

ـ الذين ينقلون عنّا الفعل الثقافي، وهم السلطة الرابعة، سلطة الإعلام، ورجال المتاعب، فمزيداً من التّغطية والتّسابق في الوصول إلى الحقيقة؛

ـ وإلى كلّ أصدقاء المخبر الذين يُشجّعوننا دائماً، وهم يحضرون نشاطات المخبر؛

ـ وإلى كلّ الطلبة بدرجاتهم، فلولاهم ما عقدنا هذه النشاطات، ونتمنى أن يفيدوا منها، ونرجو ألا يغيبوا عن أيّة محاضرة، وأقول لهم: عليكم الاستفادةَ من الحمولة العلمية والثقافية لهذه النُّخبة العلمية التي جاءتنا تزرع العلم، فاغتنموها.

أيّها الحضور، أعتذر عن كلّ من لم أذكر اسمَه، من باب المذكور يغني عن غير المذكور، ولكن من لم أذكرْه فهو في قلبي، وأقول: التمسوا لي الأعذار، وبعد؛

نعقد هذا الملتقى الوطني كما هو في عُرف مخبرنا، ففي كلّ سنة نلتقي، فلم يتأخّر المخبر سنةً من سنواته منذ تأسيسه على تجسيد الملتقى الوطني، فهذا الملتقى السادس تجري فعالياته في عنوان: **الأمن المعلوماتي: مُهدِّداته وسُبُل الحماية**. وقع

اختياره لما تعرفه تكنولوجيا التواصل من تقديم الخدمات المميّزة، وهذا ضمن الأعجوبة الثامنة، أعجوبة الشّابكة. وإشكالية الموضوع ليست تقنية بحتة، بل هي عامّة، فكان قصدُنا فيه أن تمسّ الباحثَ، ورجلَ الإعلام، والمِهني، والطالبَ والتقني والقانوني، والواعظَ... فكلّنا شريك في عمليات التطوّر التقني، وكلّنا شريك في الحذر منها لما لها من بعض المخاطر. ومن هنا، فنروم من هؤلاء الحضور أن يكشفوا عن محاسن هذه التقانات، وفي ذلت الوقت أن يُشيروا إلى تلك المُهدّدات التي لا تعمل إلاّ على التدمير الذاتي دونما شعور، ويقدموا لنا وصفات للوقاية من تلك الصدمات. وما نستهدفه من الباحثين هي تقديم سُبُل الوقاية التقنية في المقام الأوّل، ومن ثمّ هناك سُبل أخرى يمكن أن تُنشد، وعلّها تسدّ باب السطو على الملكية الفكرية وعلى الحدّ من العمل بطريقة Couper -Coller وأراها لا تعمل على تقدّم البحث العلمي، ونحن في الجامعة ينتظر منّا المجتمع أن نقدّم له مزيداً من الإنتاج النوعي، لا النقل وتلحيم المعلومات. وهنا الخطورة التي يعيشها البحث العلمي في الجامعة؛ حيث تعمل هذه التقانة –إذا لم يحسن استغلالها– على تبليد الفكر، وعلى تجسيد السطو، والبقاء ضمن دائرة الأخذ من السابق، دون الإضافة. ولكن في ذات الوقت لا ننكر أفضالها على البحث لما تقدّمه من السرعة وسهولة الوصول إلى المظان العلمية دونما جهد، وهذا ما يجب أن يُستغل لصالح الإضافات النوعية التي تعمل على أنّ اللاحق يُفيد من عمل السابق، ولا يكون صورة طبق الأصل، وهذه صفة الحضارة التي تُبنى بالإضافة.

إخواني: إنّ العالم في الآونة الأخيرة جعل موضوع الأمن المعلوماتي في صُلب انشغاله، وها هو يستنفر المختصّين ويدعو إلى التسابق في الاختراع من أجل الوقاية من المخاطر التي قد تعمل على التدمير، أو تعمل على التأخير. وقد رأينا

ذلك هماً عالمياً، وقلنا لا بدّ أن نعمل على تقديم ما يمكن أن نُسهم به في إطار خدمة الإضافة. وكان ذلك انشغالُنا منذ الملتقى السابق، وعملنا على أن ننتج أفكاراً في هذا المجال، ونقدّمها للمختصين علّهم يفيدون منها؛ لأنّ الأمن المعلوماتي جزء من الأمن العامّ، فتصوّروا لو أنّ القراصنة يصلون إلى كلمة السرّ للطيران المدني فكــم من طــائرة تسقط وتصـــوّروا لو يصـــل القراصنـــة إلى كشف حساباتنا فكم من أموالٍ تضيعُ منّا، فكيــف يتغيّــر العالَمُ في ظــروف وجيزة، فكان لا بدّ من وضع آليات الوقاية، وهذا هدفنا، فنحن نقدّر هذا التطوّر ضمن أخلقة المجتمع La moralité de la société.

إخواني: لقد عملتْ فرقة الدكتوراه بتوجيه منّي على إنتاج –معجم مصطلحات الأمن المعلوماتي) تمشياً وموضوع الملتقى، فكان المنتوج بين أيديكم وفي ظرف قياسي كبير، ومن خلاله نزعم أنّه لدينا الريادة في هذا المجال، ونتمنى من الباحثين أن يُهدوا لنا النقائص التي يسجّلونها على هذا المنتوج وهذا للتحسّن في لاحقٍ من أعمالنا عامّة. ومن خلال هذا، كان عليَ تذكير الحضور بأنّ المخبر يعيش السنة السادسة من حياته، وقام على:

ـــ 4 وحدات تأسيسية المُسمّاة CNEPRU.

ـــ 8 وحدت إضافية المُسمّاة CNEPRU.

ـــ 6 وحدات مُسمّاة PNR.

ـــ 4 وحدات تطوّعية.

ـــ 34 عدداً من مجلته الموسومة: الممارسات اللّغوية.

ـــ 16 يوماً دراسياً.

ـــ 6 ملتقيات وطنية.

ــ 10 دورات تكوينية.

ــ أكثر من 100 مطبوعٍ.

ووزّعنا عليكم الكراسة الخاصّة والمسمّاة (من التّأسيس إلى نهاية 2015) ولدينا مشاريع قادمة نأمل أن نكون في مستوى الحَدَث، ولا يكون هذا إلاّ بكلّ الباحثين وبكلّ من يُقدّم لنا نصيحة تحسينية فنحن له من السامعين العاملين على تقبّل النّصيحة.

إخواني: إنّنا في مخبر الممارسات اللّغوية نعمل من أجل النّوعية، فهناك مشاريع كبيرة مع الكثير من المُؤسّسات الوطنية، مع: مراكز البحوث، مع الشركات، مع الوزارات، مع المجلس الأعلى للغة العربة وقد شاركنا الأسبوع الماضي في ملتقى خاصّ بـــ (قسنطينة عاصمة الثّقافة العربية) وفيها قدّمت لفريقنا (ميدالية المستطيل الذهبي) وهي عربون تقدير لما نقوم به في جامعة مولود معمري من خدمات علمية لها صفة التميّز. وهناك مجهودات أخرى نقوم بها مع وزارة التّربية الوطنية ضمن تحديث المدرسة الجزائرية، ونعمل على إنجاز مشروع (مدرسة الغد، مدرسة الجودة) ونرجو أن تكلّل بالنجاح. ولا نخفي عليكم بأنّنا نسعى في كلّ مرة أن تنال جامعتُنا، والجامعاتِ الوطنية صفةَ الترتيب الدولي Le classement international من خلال صفات الجودة التي وضعتها المنظمة العالمية للمواصفات والمقاييس، وهذا ضمن مقاييس ISO ومن وراء ذلك كسبت مجلة (الممارسات اللّغوية) صفة الترتيب في الجودة، بمنحنا صفة التّصنيف والفهرسة العالمية Indexation من قبل 6 مؤسّسات شبكية عالمية، وهذا دلالة إقرار وعرفان لما تحمله المجلة من مُحتوى، وما تمتاز به الهيأة العلمية

والاستشارية من كفاءات علمية مُتميّزة. ويمكن أن نُسجّل في هذا المقام صفاتِ النوعية والعمل الأصيل، وهذا ما كنّا ننشده منذ تأسيس المخبر.

أيّها الحضور: لقد أطلتُ عليكم، واعذروني، ففي جعبتي الكثير مما يحتاج أن يُقال، ومرة أخرى أشكر كلّ من حضّر، ومن حَضَرَ، ومن سيحاضِر، وأتمنى للجميع طيب الإقامة ومتابعة الأشغال ودُمتم في خدمة العلم، وبارك الله في الجميع.

مدير المختبر: أ. د. صالح بلعيد

البرامج مفتوحة المصدر والأمن المعلوماتي

د. صديق بسّو

ج/ فرحات عبّاس – سطيف –1–

مقدمة

تعتبر البرامج الحرة والبرامج مفتوحة المصدر لبنة مهمة لتكوين قاعدة صلبة للتصدي لجميع أنواع تهديدات الأمن المعلوماتي. لذا وجب التنويه بأهميتها ونشر الوعي لدى المستعملين للتعريف بها والتعريف بخطر البرامج المغلقة. وبالتالي اختصار الكثير من الوقت والجهد في مجال الأمن المعلوماتي.

تعريف

نقول عن برنامج أنه برنامج حر إذا كانت تتوفر فيه الشروط التالية:

- حرية استعمال البرنامج لأي غرض.
- إمكانية دراسته وتعديله ليناسب حاجات المستعمل
- إمكانية نسخه
- إمكانية تطويره

هذه الشروط لابد أن تكون ممكنة من الناحية التقنية والقانونية، مما يسمح لنا أن نقول بأن المستعمل يراقب البرنامج وليس العكس.

وكأمثلة عن هذه البرامج يمكن أن نذكر: برنامج التشغيل لينكس، متصفح الواب: موزيلا فاير فوكس، برنامج الصوتيات والمرئيات: في أل سي،...

مميزات البرامج الحرة

- **إتاحة المصدر**

لكل مستخدم الحق في الحصول على الكود المصدري للبرنامج الذي يريد استعماله، حتى يستطيع تطوير هذا البرنامج وإضافة مميزات جديدة تناسب احتياجاته أو رغباته.

- **مراقبة المستخدم للبرمجية**

تتيح البرامج مفتوحة المصدر لمستخدميها تفحص الشيفرة المصدرية والتأكد من مستوى الأمن الذي توفره.

- **تنسيق حر**

لكل المستخدمين أو الذين يتعاملون مع البرامج الحرة الحق في التعاون أو تشارك الخبرات من أجل تطوير هذه البرامج.

- **مجتمعات حول البرمجية**

تعتبر البرمجيات الحرة ملكا للجميع، فهي ملك لكل من عمل على بنائها ونشر استخدامها.

- **أمن**

تتميز البرمجيات الحرة بدرع قوي مقارنة بالبرمجيات المغلقة حيث تعتبر معظم المشكلات الأمنية مشاكل عامة تختلف كليا عن تلك التي تظهر في البرمجيات المغلقة، بحيث أنه عند اكتشاف أي ثغرة أو فجوة أمنية يقوم الجميع بحلها بسرعة دون الحاجة إلى العودة إلى المطور الأساس للبرنامج.

- **إبداع**

تحفز البرمجيات الحرة المستخدمين على الإبداع في التفكير وتحسين مستوى الإبداع لدى الشباب وتغيير طريقة التفكير التقليدية.

البرامج مفتوحة المصدر

يستخدم المصطلح عادة ليشير إلى شيفرات البرامج المتاحة بدون قيود الملكية الفكرية. وهذا يتيح لمستخدمي البرمجيات الحرية الكاملة في الاطلاع على الشيفرة البرمجية للبرامج، وتعديلها أو إضافة مزايا جديدة لها.

مميزات البرامج مفتوحة المصدر

- حرية إعادة توزيع البرنامج.
- توفر النص المصدري للبرنامج، وحرية توزيع النص المصدري.
- حرية إنتاج برمجيات مشتقة أو معدلة من البرنامج الأصلي، وحرية توزيعها تحت نفس الترخيص للبرمجيات الأصلية.

- عدم وجود أي تمييز في الترخيص لأي مجموعة أو أشخاص.
- عدم وجود أي تحديد لمجالات استخدام البرنامج.
- الحقوق الموجودة في الترخيص يجب أن تعطى لكل من يتم توزيع البرنامج إليه.

أهداف البرامج الحرة

البرمجيات الحرة ليست مسألة تقنية؛ ولكنها أخلاقية، اجتماعية، وسياسية. فهي مسألة الحقوق الإنسانية الواجبة لمستخدمي البرمجيات. وبالتالي فإن الحرية والتعاون قيم أساس للبرمجيات الحرة. فعلى عكس البرامج المغلقة والتي هي برامج حكريه تشكل لغزا، البرامج الحرة تعمد الى نشر المعرفة البشرية. وفي حين ان البرمجيات الحكرية تحظر التعليم فان البرامج الحرة تدعم التعليم وتشجعه.

الفرق بين البرامج الحرة والبرامج مفتوحة المصدر

البرامج الحرة والبرامج مفتوحة المصدر هما مفهومان متنافسان لبرامج ذات خصائص متطابقة

البرامج الحرة: تعطي أهمية كبرى للجانب الفلسفي والسياسي

البرامج مفتوحة المصدر: تعنى بطريقة التطوير والنشر

أفكار من مدرسة ريشارد ستالمان

يعتبر ريتشارد ستالمان الأب الروحي للبرامج الحرة، في هذه الفقرة نذكر بعضا من التوجيهات العملية التي يذكرها في جملته المشهورة: لماذا يجب ألا تستعمل (لا تُستعمَل: لا تدعه يستعملك).

جوجل

- أغلب خدمات جوجل تتطلب برامج مغلقة المصدر مثل (Javascript)، إذا رفضت استعمالها ولجأت بدل ذلك الى برنامج حر مثل (Libre JS) فستلاحظ أنه لا يمكنك استعمال الخدمة

- التعريف بنفسك في خدمات جوجل يعتبر خطأ كبيرا يجعلك تحت المراقبة
- برنامج (Gmail) مصمم لإنشاء نموذج نفسي لكل مستعمل وحتى لكل مرسل

سكايب

يستعمل سكايب برنامجا مغلقا على مستوى الزبون، مما يعني أنه يراقب المستعمل

- يمكن لسكايب أن يطلع على المكالمات
- قامت شركة سكايب بإعطاء معلومات خصوصية عن أحد متتبعي ويكيليكيس
- يمكن لميكروسوفت الاطلاع على رسائل سكايب

بدل ذلك يمكن استعمال: Ekiga, Mumble, Jitsi

فايس بوك:

- تمارس فايس بوك رقابة كبيرة على المنشورات، اذ قامت بحجب الكثير من الصفحات لأراء سياسية أو فكرية
- إذا أصبح الموقع الأول للصحافة فسيكون نقطة تفتيش للأراء والأخبار
- التعرف الالي على الصور ومراقبة الأشخاص
- يمكن لفايس بوك إعطاء معلوماتك الشخصية

خاتمة

بعد معرفة أهمية البرامج مفتوحة المصدر، وخطر البرامج المغلقة من حيث الأمن المعلوماتي، إذ يمكنها التجسس على مستعملها أو القيام بمهام أخرى غير المصرح بها لابد من التوصية بتشجيع استعمال البرامج الحرة سواء من طرف الأفراد أو المؤسسات خصوصا وأنه يوجد مقابل من البرامج الحرة لكل برنامج مغلق.

المراجع

البرمجيات الحرة والتعليم، نظام التشغيل غنو، www.gnu.org

الصفحة الرسمية لريتشارد ستالمان.

ويكيبيديا: مصدر مفتوح– برمجيات حرة –Open source - Logiciel libre

الأمن اللغوي منطلق للأمن المعلوماتي
- مهدداته ومستلزماته-

د/ حسنية عزاز

جامعة جيلالي اليابس، سيدي بلعباس-الجزائر

الملخص: كثُر الحديث عن الأمن اللغوي، ونحن لم نعهده في شقه الأول إلاّ حينما يتعلق الأمر بالحرب أو الجوع، فنقول: الأمن العسكري والأمن الغذائي، لما لهما من أهمية من أجل الحياة والاستمرارية، فتؤمن النفس غذائيا وعسكريا؛ لكن مصطلح الأمن اللغوي ظلّ الشائع السائد اليوم في أوساطنا اللغوية، ومع باحثينا كبارا أو مبتدئين.

فالكلّ يحاول أن يؤمن لغته ويحافظ عليها لكي لا تدوس عليها أقدام اللغات الأخرى، وتنتقل من لغة حية إلى عداد اللغات الميتة، ويبقى السؤال مطروحا، هل حققنا هذا الأمن اللغوي الذي طالما تحدثنا عنه، واجتمعنا لأجله، ووضعنا له خططا وتخطيطا في ملتقياتنا، ومؤتمراتنا الوطنية والدولية؟ أو بالأحرى هل حاولنا تحقيقه بتطبيق ما أوصي به في تلك اللقاءات؟

أنا لا أدّعي – في هذه الورقة البحثية- أنّني سأقدّم خطة شاملة جامعة مانعة للأمن اللغوي، لكي يفيد بها العالم مدى الحياة، بل أريد أن أقدّم رأيا لعلّه يضاف للآراء الأخرى السابقة لي والحاضرة معي وربمّا المستقبلية، لمعرفة المستلزمات الحقيقية للأمن اللغوي، فهو يشبه إلى حدّ بعيد الأمن العسكري الذي يحتاج إلى عسكر وعتاد وخطط وجاهزية وفطنة ويقظة وثقة وتضحية حينما تقتضي الضرورة ذلك، وحينما يؤشر للخطر وتعلن صفارات الانذار عنه.

إذن لا بدّ من كل هذه المواصفات، هذه المستلزمات، فهل هي نفسها التي نتسلّح بها؟ لنقول: أنّنا قد حققنا – عمليّا– أمنا لغويا. هذا ما سنجيبكم عنه – إن شاء الله– فيما ما يلزمنا لنحقق الأمن اللغوي.

الورقة البحثية: إنّ حصافة هذا الموضوع تكمن في علاج قضية من أهم القضايا اللغوية (الأمن اللغوي)، فقد ظهر الاهتمام بها مؤخراْ في الكثير من الثقافات العالمية؛ لأنّ هذا الأمن يستهدف الحفاظ على اللغة وصولا إلى الحفاظ على الهوية، والأمن من التبعية والذوبان والاستيلاب بين الشعوب.

وإلى جانب ذلك يُعدّ الأمن اللغوي عنصرا مهما من عناصر الأمن الاجتماعي؛ لأن اللغة الواحدة الموحدة هي الرابط الأقوى بين فئات المجتمع الواحد، وهي وسيلة التواصل والتفاهم بين أبناء الهوية الواحدة؛ لذلك فإنّه لا هوية بلا لغة[1] والهوية التي تجمع العرب من المحيط إلى الخليج، أكدّتها اللغة العربية، التي لولاها لضاعت المعالم، ومن هنا كان الحرص عند كثير من الأمم على العناية بلسانها وتنقيته من كل ما يشوبه، والواقع أن ما آل إليه اليوم حالنا أشبه بارتداد عن الاهتمام باللغة العربية نطقا وكتابةً، بعد أن كان الإقبال عليها هو الأصل، ولذا وجب علينا الاهتمام بها، بل رسم معالم واضحة مستقبلية تحفظ لها قواعدها وترمم لنا أركانها.

إذن لا بدّ من أمن لغوي حتى لا تضيع منّا هذه اللغة، ولنحميها من الدّمار والحوادث اللغوية الدخيلة، إنّه مطلب ضروري حرصت عليه الكثير من الأمم والشعوب، فدعّمت أمنها اللغوي، وذلك بتحصينه من الاقتحامات والخروق؛ لدحر الدخيل المنافي لطبيعة تكوينها[2]، ومن الدول من اعتبرت أمنها اللغوي عنصرا مهما في منظومة أمنها القومي[3]، لنكن... نحن كذلك، لقد حان الوقت لنسترجع الثقة في أنفسنا وفي لغتنا ونحقق الأمن للغتنا والآمان لنا، ويبدو لي– قبل الحديث عن الأمن اللغوي– أنّ ثمة **مهدّدات** تهدده، وبإدراكها ودراستها نخلص إلى وسائل الوقاية، وقد أسميتها **المستلزمات**. لكن المهددات التي سأذكرها ليست بالضرورة

كلّها أو أهمها، وإنما ما أراه اليوم – ومن وجهة نظري– أنها أبرز ما يهدد الأمن اللغوي، وقد أتيت إلى ذكر بعضها، أمّا عن المستلزمات، فهي عديدة وناجعة ذكرت أبرزها أيضا.

وإليكم مهددات ومستلزمات الأمن اللغوي في هذا التّحليل:

أــ مهدّدات الأمن اللغوي:

1ــ ضعف أداء اللغة العربيّة؛

2 ــ طغيان اللغات الأجنبية؛

3 ــ التهجين اللغوي؛

4 ــ ضعف أداء لغة الإعلام؛

5 ــ تعاملنا مع العولمة في جانبها السّلبي؛

6 ــ التّفريط في الهُوية وفي الخصوصية؛

7 ــ سوء تدبير ثقافة الاختلاف؛

ب ــ مستلزمات الأمن اللغوي:

1 ــ تفعيل العربية في التربية والتعليم؛

2 ــ حفظ الحقوق اللغوية للطفل؛

3 ــ التّعــريب؛

4 ــ الوعي اللغوي؛

إنّ اللغة هي وعاء الفكر ومرآة الثقافة[4]، وأداة التفكير، كما أنها من أهم ملامح الشخصية الإنسانية؛ لأنها تربط المرء بأمته وثقافته ودينه وتحدد هويته، واللّغة تجميع لتلك الأفكار، ولذلك تعمل الشعوب المتحضّرة على توحيد لغة التواصل الاجتماعي ليحصل ذلك الانسجام الجمعي وتحصل التنمية البشرية، من خلال تخطيط السياسة اللغوية المبنية على الاستراتيجية الشاملة ذات الأبعاد الثلاثة المستعجلة، و قصيرة المدى، وطويلة المدى، إضافة إلى التخطيط التربوي الذي تُستَقى موضوعاته من التخطيط اللغوي.

وقبل التفصيل في الأمر، أريد تحديد بعض المفاهيم ذات العلاقة بالموضوع- على حد قول المفكر الفرنسي فولتير" voltaire" (1778): إذا أردت أن تتحدث معي فحدّد مصطلحاتك- ومنه نحدد المصطلحات الأساس لعنوان البحث والمتكونة أساسا من أربع وحدات لغوية هي: مهددات، مستلزمات، الأمن، اللغوي.

1- مهددات: هي تلك التهديدات أو الاعتداءات الداخلية أو الخارجية، والمظاهر التي تخترق أمن اللغة.

2- مستلزمات: هي وسائل الوقاية والحماية من المخاطر التي تحيط باللغة وهي متطلبات الأمن اللغوي.

3- الأمن اللّغويّ: من الأمان: أَمَنَة وأَمْنٌ[5]، ومعناه الاطمئنان، ومبالغته أُمَّان: رجل صوّام.. حتى قالوا من حمامِ مكّةَ، وقال الله تعالى:﴿ وضرب الله مثلا قرية كانت آمنة مطمئنة يأتيها رزقها رغدا من كل مكان فكفرت بأنعم الله فأذاقها الله لباس الجوع والخوف بما كانوا يصنعون﴾[6]، وقال تعالى:﴿ ثمّ أنزل عليكم من بعد الغم أمنة نعاسا يغشى طائفة قد أهّمتهم أنفسهم يظنون بالله غير الحق ظن الجاهلية يقولون هل لنا من الأمر من شيء قل إنّ الأمر كله لله ﴾[7]، والأمن هو الطمأنينة وذهاب الخوف والسلامة من الشر، وأمِن الرجل اطمأن ولم يخف، وأمِن الرجل على كذا: وثق به، اطمأن إليه، أو جعله أمينا عليه، قال تعالى: ﴿هل آمنكم عليه إلا كما أمنتكم على أخيه من قبل﴾[8] فاللّغة أمانة؛ ولا بدّ من المحافظة على هذه الأمانة بأمنٍ على غرار ما فعل أسلافنا في العصور الأولى للدولة الإسلامية حينما عمموّا الأمن اللغوي بسُلطة العلم والمعرفة، حيث وقعت الحكمة على لسان العرب بالأصالة اكتسابا، وبالاستعراب تعلّماً وقناعة، فكانت العصبية العربية مفتاح الحضارة؛ كما كان الأمن اللغوي حضارة وبناء وتعميراً، وكان الأمان أساسَ المُلْك[9].

ويمكن تعريف مفهوم الأمن اللغوي بالآتي:

هو إحاطة اللغة بسياج من الحماية الرسمية (من خلال القرارات السيادية الوزارية والإدارية) وغير الرسمية المعنوية والمادية بوضع الأنظمة والضوابط الملزمة للأفراد والمؤسسات التي من شأنها أن تصد كل التهديدات والاعتداءات التي تستهدف أمن اللغة العربية وسلامتها بقصد أو بغير قصد، سواء أكانت هذه التهديدات أو الاعتداءات داخلية أم خارجية[10].

والأمن اللّغويّ (la sécurité langagière) نظرية تتعلق بموضوع استعمال اللّغة وحمايتها بشتّى الأساليب، ومختلف الطرق المنهجية، غير أن هذا الأمن تهدده مهددّات ولعلّها لا تخرج عمّا سأذكره في العنصر التالي:

2-<u>مهدّدات الأمن اللّغوي</u>: لكي يحصل الأمن اللّغويّ، علينا إدراك مهدداته ودراستها للخروج بوسائل الوقاية. ومن المهددات -ما يكون مصدرها أهل اللغة مثل: أفراد المجتمع، والمؤسسات والشركات، أو مصدرها من غير أهلها- ما يأتي:

2-1- ضعف أداء العربيّة: لم تعد العربية لغة العلم في واقعنا الاستعماليّ، مثل ما كانت عليه في زمن الدولة الاسلامية في قرونها الغرر (أيام الرشيد والمأمون وغيرهما)، فهي لا تُمارَس في الأُسرة ولا في المحيط، ولا يحصل فيها تطوير في مناهجها إلاّ في الأمور السّطحيّة، كما حُكِمَ عليها بالاستخدام في الفصول الدراسية فقط، أو في المخاطبات الرسمية في مجالات العمل مع التهاون في تعلمها والتقليل من أهمية استخدامها وإتقانها.

2-2-طغيان اللغات الأجنبية: وهذا ما هو حاصل في كلّ الدول العربيّة، ولغة المستعمر هي الفضلى، والتي تنال مقامها في دواليب الدّولة، بالرغم ممّا تنص عليه النصوص والدّساتير والمواثيق ومختلف النّصوص التشريعيّة من مقام اللغة الرسميّة، مثل شيوع استعمال اللغة الفرنسية في أوطان المغرب العربي، فكثير من الاتفاقيات والقرارات تسيّر وتكتب مراسيمها باللغة الفرنسية، وتأسيس الجرائد المكتوبة بالأجنبيات والمفروض أن توجه للجاليات الأجنبية فقط لا إلى الشعوب

العربية علما أنّ اللغة العربية في وقت الاستعمار الفرنسي كانت المكوّن الرئيس للوطنية وللحركة التحررية الجزائرية، والحديث نفسه عن الثورات المغاربية الأخرى ضدّ الاستعمار الفرنسي. وقد تغير الحال بعد الاستقلال، فترى مجموعة من النخب المثقفة لا تريد بديلا عن الفرنسية ولا حوارا عن المسألة اللغوية[11].

2-3- التّهجين اللّغوي: هو واقع جديد صاحب التكنولوجيا والتقنيات الحديثة يفرض المزج بين اللغات المحلية و اللغات الأجنبية أو العربية الفصحى، وهذا ما هو حاصل الآن في وسائط التواصل الاجتماعي من كتابة الرسائل(sms) بالحرف الأجنبي والمضمون العربي الخليط، فالبعض يعمد إلى هذا النوع من الكتابة لضعف في مهارة التحرير الكتابي أو الإملاء، والبعض الآخر يرى أن الكتابة بالحروف اللاتينية أسرع وأسهل، وآخرون يعزون ذلك لعدم إتاحة اللغة العربية في كل المنتجات الالكترونية كالأجهزة الحاسوبية والهواتف المحمولة والأجهزة اللوحية...إضافة إلى استخدام الناطقين باللغة العربية لغة ثانية في التواصل في ما بينهم خاصة استعمال بعض المصطلحات والتعبيرات التي اعتاد عليها الناطقون بالعربية ظنا منهم أن ذلك يسهل عملية الفهم والإفهام ويسرع توصيل الرسالة.

2-4- ضعف أداء لغة الإعلام: للإعلام بمختلف وسائله (المرئية والمسموعة والمقروءة) أهمية كبيرة لما لها من تأثير قوي في عقل ووجدان المتلقي، فهو يتأثر بالمضمون والشكل من لغة ورسومات وإشارات، وفي هذا المقام وفي حديثنا عن اللغة، نطرح السؤال: أي لغة تتداولها الصحف والمجلات والقنوات؟ فإذا سميناها لغة، في أدنى مستويات اللغة الفصيحة بل إنّها هجين وإهمال كامل للفصحى خاصة في البرامج المباشرة، وهذا يهدد الأمن اللغوي.

2-5- تعاملنا مع العولمة في جانبها السّلبي: إنّ العولمة التقاء الحضارات والعولمة هي الاستفادة مِمّن هم أفضل منّا علماً ودراية، والأخذ عنهم بإدخال تكييف يراعي الخصوصية، ولذا كان علينا اكتساب خبرات الغرب من بابها الواسع، بدءاً من المُنجزات المادية إلى الخبرات وكيفيات الإنتاج؛ لنحتكمَ عند ذلك

بالتّصرّف والتّكيّف مع "ظاهرة العصر وسمته، وأنّ الوقوف في وجهها أو محاولة تجنّبها أو العزلة عنها، إنّما هو خروج على العصر وتخلف ما وراءه. وعلينا أن نسارع إلى دراسة عناصر هذه العولمة، وفهم مكوناتها والتّنبيه لاتّجاهاتها، ثمّ علينا أن نتعامل معها من موقع الثقة بالنّفس والإدراك العميق لخصائص ثقافتنا واستخراج كوامنها الأصيلة وجواهرها الحقيقية، وتعريضها للتفاعل مع تلك الثقافة العالمية الواحدة: أخذ وعطاء. ولا يجوز لنا أن نقف مكتوفي الأيدي، عاجزين عن القيام بعمل حقيقي وفعل أصيل"[12]. إنّ العولمة تعني في ما تعني العالمية، كما تعني أيضاً التّغيير الإيجابي، وملاحقة مُستجدات العصر، لا التغيير السلبي والانصهار في الآخر.

لا يمكن أن ننكر أنّ خطابَ العولمة يظهر فيه بعضُ الفَرْض، أو هو خطاب حتمية في بعض المقامات، ولا خيار للضّعيف إلاّ الانصياع له، وإلا فمصيره الانقراض، هذا موجود بالقوّة، ولكنه ليس موجوداً بالفعل، فهناك مُناداة بالحفاظ على الهُوية في إطار عدم تفسّخها، وعدم كون الفرد نسخةً لغيره، خُلُقاً وخلقة ولسانا، بل يجب المحافظة على الهوية، ومن تمثلاتها اللغة، وننسى وهم اللغة الانجليزية هي اللغة العالمية، ويتسارع الناس والشباب منهم على التداول اليومي لبعض الألفاظ كمظهر من مظاهر الرقي الاجتماعي.

2-6- التّفريط في الهُوية وفي الخصوصية: إذا هُدِّد الإنسان بشيء فعليه المواجهة وإلا العزلة والاختباء فالانقراض شيئا فشيئاً، هكذا هي العولمة، إذا كانت تهدّدني، فإنّها تتطلّب منّي المواجهة، ويبدو لي بأنّ مواجهة العولمة بالهُوية والتّميّز والنديّة ممكنة، ولكن المواجهة الحقيقة للعولمة تكمن في إعطاء الأولية للإصلاح الاجتماعي المصحوب بالمشاريع التّعليمية والتّثقيفية والتّنموية والنّهضوية، دون الخروج عن السّرب أو الجماعة.

إنّ العولمة نهضة حضارية توقظنا وتعمل على تحريكنا برجّة قويّة كي نكون في هذا الكون، وننال موقعنا في الأرض، فهل تحتاج إلى مواجهة؟ أو ما هي

المواجهة المطلوبة لمن يعمل على إنهاضنا، فإذا قبلنا بالمواجهة، نعود إلى نقطة البداية، لماذا تأخّرنا وتقدّم غيرُنا؟

وإذا كانت العولمة تعمل على إضعاف الهُويات القومية، ومحو صفات التميّز للشّعوب الضّعيفة وفرض الثّقافة القطبية وسيطرتها، وهُويتنا –نحن العرب– ليست مُحصّنةً في هذا الجانب، وبخاصّة في عدم التّواصل بلغتنا في كثير من الجوانب؛ ويعني افتقاد الانتماء والهُوية، وهذه مشكلة داخلية فرضها العربُ على أنفسهم؛ حيث لا يريدون التّواصل بلغتهم، فليس الأمر يعود للعولمة، بل إنّ العربية لها موقع مُتقدّم بين لغات العالم العَشْر، ولكنّ العربَ لا يريدون ذلك، فهم يتسامحون في أهمّ ركيزة في الهُوية، وهي الهُويّة اللّغوية، ولا يدرون أنّه لا هُويّة عربية بدون لغة عربية، ولا لغة عربية بدون هُويّة عربية.

ومن هذه الهُويات "هُويّة مجتمعنا العربي مُتمثّلة في لغته التي تعد محور ثقافته ومن ثمّ فإنّ الخطر ينصبّ على اللّغة، وما كانت اللّغة والهُوية إلاّ وجهين لعُملَة واحدة، فهما خاصيتان إنسانيتان والإنسان في جوهره ليس إلاّ لغة وهُوية، اللّغة فكره ولسانه، وفي الوقت نفسه انتماؤه وتلك هي حقيقته وهُويتّه"[13]، وتبقى العربيةُ أهمَّ عاملٍ باعتبارها هُوية ثقافية مُوحّدة تعمل على الانسجام الجمعي، وتؤدّي إلى الأمان لأنّها الحاضن والمعبّر عن الثقافة والحضارة والقيم والأخلاق التي تعاملَ الناطقون بها.

إنّ الهُوية حالة من التفرد والخصوصية التي تلامس المستوى القيمي والعقائدي للأمة[14] وملمح من ملامح شخصية الإنسان وتُعطي له صفة التّميّز بين النّاس والعلاقة بين اللغة والهوية علاقة ارتباط واضح ووثاق لا جدال فيه، ومن فرّط في لغته، يعني فرّط في هُويته، مثلما فعل العرب بلغتهم وقبلوا بالتّعدّد اللّغوي الأجنبي ونعرف أنّه عندما تتعدّد الهُويات تنقلب إلى تفتيت في الأذهان، وهو مدخل إلى تفتيت في الأوطان، فتُمَّحى الخصوصية التي تحمل معنى المواطنة والوطنية

فالهُوية لا تكون ثابتة، بل إنّ الهُوية تقبل الأخذ كما تعطي، فهي انفتاح وتأثير وتأثر، مع الحفاظ على الخصوصية دوما.

2-7- سوء تدبير ثقافة الاختلاف: ليس معنى الاختلاف هدم للخصوصية بل هو ابتعاد عن التعصب للرأي الواحد، ولا يتعلق الأمر بالمبادئ والأصول التي لا جدال ولا خلاف ولا اختلاف فيها، وإنما في الاختلاف تجدد فكر وتعدد آراء وإنتاج أفكار جديدة تخدم هذه الخصوصية.

والخصوصية في الأمن اللّغوي؛ هي إعادة الاعتبار للغة العربية والوفاء باستحقاقاتها الأساسية، والتّشجيع على دراستها وتطويرها وترسيخها، وجعلها قادرة على التّعبير عن كلّ المُتطلبات الحياتية، وجعلها مُتفاعلةً مع اللّغات الأخرى لا في صراعات معها، فالتعدّد اللّغوي مقبول وجيّد، مع الحفاظ على اللغة الرسمية وممارساتها في مختلف المجالات التي سنّها لها الدستور؛ أي المحافظة على حقوقها مع العمل على معاملة اللّغات الأجنبية كلغات أجنبية؛ أي أن تحصل الاستفادة منها، لا أن تنافس اللّغات الوطنية -كما هو مشاهد اليوم- في المعاملات الرسمية والعادية. وبكلّ أسف لم نستطع الخروج من شرنقة لغة المستعمر القديم بل لم نستفد من تجارب الشّعوب الناجحة التي خرجت من لغة المستعمر بأقلّ الخسائر، بل أبدعت بلغاتها وفي لغاتها، وحصل لها التقدّم عمّا كانت عليه أيام استعمال اللّغة الأجنبية[15].

إذن تتعدد مظاهر الاختراق اللغوي غير أن وسائل الأمن اللغوي التي تسهم في سلامة اللغة العربية وحمايتها موجودة وممكنة التطبيق، فما هي هذه المستلزمات:

3 ـ مستلزمات الأمن اللغوي:

3-1- تفعيل العربية في التربية والتعليم: تحتاج العربية في هذين الميدانيين إلى نظرة جديدة ثاقبة في المنهج وطرق التدريس، وإذا أردنا فعلا أن نفعِّل العربية في التربية والتعليم علينا إلزام المتعلمين بتعلمها وإتقانها في المراحل الأولى وتأخير تعليم اللغات الأجنبية إلى ما بعد التحكم في آليات لغته، ومن ثمّ نطلق له

حرية الاختيار في اللّغات الأجنبية من أجل اكساب المتعلّمين المهارات اللغوية إرسالا واستقبالا، وبالتالي تنمية أساليب التفكير لديهم بمنهجية بعيدة عن التشويش- وأقصد بذلك أنه يدرس بلغة ويفكر بلغة أخرى- .

ومن أجل التمكين الفعلي للعربية في التربية والتعليم يجب غرس روح المواطنة اللغوية، فللمدرسة دور ترسيخي في إعطاء المعارف العلمية، وفي دفع التلاميذ لخدمة مجتمعاتهم، والاهتمام بالمواطنة الصالحة تولي اللغة الرسمية/ اللغة الوطنية/ الثقافة الوطنية كلّ الأهمية، وتجسيد المواطنة اللغوية، التي هي استعمال اللسان الوطني في كلّ المؤسّسات والأماكن العامة، وفضاء المصالح الإدارية. وإنّ المواطنة اللغوية فضاء لغوي ممتدّ تأخذ فيه اللغة الرسمية النصيب الأوفى انطلاقاً من أنّ تربية المواطنة تحصل أولاً باللغة الرسمية، وعدم احتقار الوطنية، وتعزيز الثقافة الوطنية بنقل المفاهيم الوطنية للطفل، وبثّ الوعي بتاريخ الوطن وإنجازاته والاهتمام بمختلف الأنشطة الثقافية، وخاصة الثقافية التي تنسج في الغالب علاقة مميزة بين المواطنين، بتحسيسهم أنّه جزء من ذواتهم "فالعلاقة بين مفهوم المواطنة ومفهوم الثقافة الوطنية هي علاقة مشاركة إبداعية في خلق فضاء وطني جديد متجدّد يتجنّب العزلة والانكفاء ويحارب التعصّب والشوفينية، ويؤسّس للاندماج والوحدة على قاعدة الديمقراطية واحترام التعدّد وصيانة حقوق الإنسان[16]". وهكذا فإنّ المواطنة اللغوية لا تجئ مفاهيمها المرتبطة بالحقوق أياً كانت، بل تحتاج إلى تجسيد فعلي في حقّ التلميذ في تعلّم لغته، وحقّه في استعمال لغته وإدخالها إلى منظومة اللغات الحية، وحقّه في أن تدافع مؤسّسات الدولة على نيل المرتبة التي تستحقها كلغة رسمية/ وطنية، وتسنّ القوانين العاملة على احترامها.

3-2- حفظ الحقوق اللغوية للطفل: حقوق الطفل معروفة، من بينها الحقوق اللغوية المستقاة من البيان الذي أصدرته اليونسكو عام 2007 بمناسبة الاحتفال بيوم اللغة الأمّ المصادف 21 فيفري من كلّ عام، وأكدّ البيان أنّ الحقّ اللغوي من ضمن حقوق الإنسان، وأنّ من حقّ كل طفل أن ينعم بلغة الاكتساب الأمومي

وبلغة التداول الجماعي، وبلغة التحصيل المعرفي[17] ومصطلح الحقّ يعني أن تتكفل الأنظمة باللغة الأم في كلّ أبعادها التعليمية، ولغة الطفل المعنية هنا هي اللغة العربية الفصحى.

إذن لا بد من حفظ هذا الحق للطفل، الذي من خلاله نحافظ على اللغة العربية فقديما قيل: "التعلّم في الصغر كالنقش في الحجر" وقال الشاعر:

قد ينفع الأدب الأولاد في صغر   وليس ينفعهم من بعده أدبُ

إنّ الغصون إذا عدلتها اعتدلت   ولا تلين-لو ليّنته-الخشبُ

للطفل حقوق في تعلّم لغته الأم وتعلّم اللغات الأجنبية، لذلك لا بد من وضوح الأهداف العامة للمنظومة التربوية، بوجود برامج تعليمية تواكب آليات العصر ولا يتأتى ذلك إلاّ بتخطيط تربوي وسياسة لغوية واضحة المعالم.

اللغة جزء مهم من حياة الطفل وشعوره، واكتسابها يكون في البيت والمدرسة والبيئة، وكذلك في وسائل الإعلام، ولما للغة في هذه المرحلة من الخطر والأهمية ولكون اللغة هي أجلى مظاهر الانتماء والهوية؛ كان لزاما أن تضبط الوسائل التّي تؤثّر في مستوى إدراك الطفل لها، وأن تُسنّ قوانينُ ويُعمل على تقديم اللغة تقديما فصيحا صافيا، وهذا حق مشروع للطفل.

3-3- التّعريب:

هو استبدال للغات الأجنبية السائدة في مختلف دواليب الدول العربية باللغة العربية، وبخاصة في التربية والتعليم. ولذا جاءت كلمة (التعرّيب) من عرّب. وهذا ما تقوم به الدول العربية عن طريق المؤسسات التي وضعتها مثل المدارس والجامعات، والمجامع اللّغويّة.

ومؤكد أنه من وسائل الأمن اللغوي العمل الجادّ لتعريب التعليم والعلوم المختلفة وتدريسها في مراحل التعليم قبل الجامعة ثم المراحل العليا. (مثل تجربة الجامعات السورية بتدريس علوم الطب والكيمياء والرياضيات الحديثة والفيزياء والجيولوجيا وعلوم الذرة والفضاء والطب النووي والصناعات الكيماوية والهندسة وغيرها بلغة

عربية خالصة) فالعربية غير قاصرة في استيعاب العلوم وحضارة العصر، إنما القاصر عن التقدّم هم أهلها والناطقون بها.

وكذلك لا ننسى دور مجامع اللغة العربية في التشجيع على التعريب حيث رأى مجمع اللغة العربية في القاهرة أن: "للتعريب في عصرنا الحديث فوائد تتلخص في غنى اللغة بذخيرة من الكلمات التي تعبر عن كل ظلال المعاني الإنسانية كما أنه يمدنا بفيض من المصطلحات العلمية الحديثة التي لا نستغني عنها في نهضتنا العلمية"، فضلا عن عقد العديد من المؤتمرات والندوات ومنه المؤتمر العاشر للتعريب الذي عُقد في دمشق برعاية المنظمة العربية للتربية والثقافة والعلوم تحت شعار " قضايا تعريب التعليم العالي في الوطن العربي" في 2002م ، حيث خرج المؤتمر بمجموعة من التوصيات منها "الحرص على احتواء كل كتاب علمي منهجي على مسرد أجنبي عربي وعربي أجنبي يضم كل المصطلحات العلمية الواردة فيه، ووضع الكتب العربية التي طبقت التعريب بين يدي الجامعات والمؤسسات، ودعم الطباعة المعجمية وأبحاثها ومشروعاتها التي تخدم قضية التعريب كمشروع الذخيرة اللغوية ومشروع المعجم الصحفي العربي المعاصر ومشروع يقيس المصطلح وغيرها من المشروعات المعجمية[18].

3-4-الوعي اللغوي: إنّ الوعي اللغوي هي القيمة العليا للتاريخ الإنساني باعتباره ليس هو الحضارة المادية كمكان، وإنّما هو الحضارة الروحية في كلّ زمان ومكان، فهو الذي يحرّرنا من أوهام عالقة في مخزون ذاكرتنا الجمعية ويعمل على إثبات أنّ الوجود حقيقة جمالية ثابتة، وأنّ الأشياء لها وقعها وأنّ اللغة لم تكن عبثاً، بل لها صيغة تحريضية ترتبط بجدلية ما خلفه الأجداد، وما جادت به الأوقات. ولا جدال في أنّ النهوض العقلاني يتطلّب وعياً لغوياً منفتحاً على حقائق ذاتية مستترة، أو مسكوت عنها، فبقدر ما ينمو الوعي اللغوي باللغة الوطنية تكبر الحضارة ونكبر فيها وبها، ولا غرو كذلك في أنّ كلّ أنواع الدراسات اللغوية التي تبحث في الوعي هي عملات إفصاح عن مستنبطات النفس منطلقاً من أنّ جوهر

الوجود هو الجوهر المعرفي للذات، وكانت معظم الشعوب تتّخذ من الوعي اللغوي أبرز مقوّمات وجودها الروحي والمادي، والوعي بأهمية اللغة الوطنية هو الذي يضمن **الأمن اللغوي** في مرحلة التطوّر العلمي والمعلوماتي، وتعدّد وسائل الاتّصال، والحوار الذي لا يحصل به الإلغاء إلاّ بوعي الذات لخصائصها التراثية والمستقبلية "حوار ينبني على الوعي بالذات والوعي بالآخر لفهمه والاقتراب منه ويتحلّى بالموضوعية وحسن النية، هو وحده الكفيل بتدعيم هذه المسيرة من التحدّيات وهو الوحيد الذي يشهد المتقبل بمصداقيته وجدواه[19]. وإنّ الوعي اللغوي يمكننا من فهم العالم وتملّكه معرفياً، والوعي لا يحصل إلا بمعرفة ما يمكن أن تحقّقه اللغة الرسمية/ الوطنية من تطوّر حضاري، وكيف تجعل المجتمع منتجاً وليس مستهلكاً فقط، ويا ليت أقوامنا يعلمون ما في العربية من حماية لكلّ أشكال الثقافة الوطنية، وهي أساس كلّ نضال وبُعد لغوي ووطني، ومن ليس له بُعد لغوي ووطني ليس له بُعد معرفي، وبالتالي ليس له بُعد ذاتي، وليس له استقلالية.

خاتمة: إنّ اللغة العربية هي اللغة الرسمية في سائر الدول العربية، ولئن لم تكن اللغة الوحيدة المستخدمة في عدد من البلدان العربية تتعايش معها لغات وطنية أخرى، ولغة أجنبية، فإنّ لها منزلة خاصة اكتسبتها بفعل التاريخ والحضارة العربية الإسلامية التي عمّت بلادنا بالذات. واللغة العربية مؤسّسة اجتماعية رئيسة ذات دور محوري في تماسك المجتمع وتواصله وتحقيق تنميته الشاملة؛ السياسية منها والثقافية والتربوية والاجتماعية والاقتصادية، لذلك تعدّ من مؤسّسات السيادة ومحلّ اهتمام الجميع، أو هكذا ينبغي أن تكون.

تحتاج اللغة العربية، كسائر اللغات إلى عناية متواصلة، وإلى ترقية منظّمة لتحسين أدائها والحفاظ على سلامتها وزيادة الاعتزاز بها. وإنّ هذه الترقية تقتضي أن يعيَ الجميع ضرورة المحافظة عليها والمساهمة الجادة في تحسين مردودها والعمل على نشرها والدفاع عنها، ممّا يعدّ شرطاً ضرورياً لترقيتها. وهذه الترقية تهمّ مختلف مجالات اللغة من: نحو ومعجم ومصطلح وتعبير، كما تهتمّ بتطوير

طرائق تعليمها، وأساليب نشرها عبر وسائل الإعلام الجماهيري، وتقانات المعلومات والاتّصالات الحديثة. على أنّ ترقية اللغة العربية تستلزم – بالإضافة إلى إجراء البحوث اللغوية الجادة التي تذلّل كثيراً من العقبات– سنّ التشريعات وإصدار القوانين التي تنظمّ علاقة المواطنين بمختلف المؤسّسات؛ ذلك أنّ ترقية متن اللغة أو سنّ التشريعات أمران متلازمان، ولا نجاح لتلك الترقية بدونهما معاً وهذا ما أثبتته تجارب رائدة شرقاً وغرباً.

كما ينبغي أن يسود بيننا حوار ثقافي صحيح، حوار يدعّم مسيرة البلاد العربية في مواجهة تحدّي العولمة في شقّها الاقتصادي والثقافي والإعلامي، وبقدر يحصل الحوار ستترسم المعالم الهوياتية وتقوى والسعي لتكريس هذا الحوار عن طريق **منظومة القيم** التي تأتي من **البيت والمدرسة.** ومن هنا نقول أننا حققنا **الأمن اللغوي.**

التوصيات:

1. – الاهتمام بمنظومة التّربية والتّعليم أهميّة وتطوير مناهجها.

2. – التطبيق الفعلي لقرار التعريب الشامل.

3. – الاستفادة من التّجارب النّاجحة لدول أخرى في المجال اللغوي وأخذ العبرة منها.

4. – تفعيل المجامع العربية والمؤسسات اللغوية لإيجاد حلول للأزمة اللغوية.

5. - الخروج بقرار عربيّ بخصوص القضايا اللغوية المشتركة، نحو: المعجم التاريخي للغة العربية والذخيرة العربية، والعمل على تحقيق هذه المشاريع الكبرى **لتحقيق الأمن اللغوي.**

الهوامش:

---

1 – ينظر: أ.د. أحمد محمد الضبيب، نحو أمن لغوي، أعمال الملتقى العلمي "دور التعليم والإعلام في تحقيق أمن اللغة العربية" مركز الملك عبد الله بن عبد العزيز الدولي لخدمة اللغة العربية، الرياض: من 14ـــ1435/11/16هـــ الموافق لـــ09ـــ2014/9/11م، ص11.

2 – ينظر: منير الحافظ، الأمن اللغوي وتحديات الحداثة، مجلة الموقف الأدبي – مجلة أدبية شهرية تصدر عن اتحاد الكتاب العرب بدمشق– العدد 433 آيار 2007م، ص51.

3 – ينظر:د. سعيد بن مسفر المالكي، الأمن اللغوي في المملكة العربية السعودية" النظرية والنموذج"، مجلة اللغة العربية آفاق فكرية، خوارزم العلمية للنشر والتوزيع، ط1 1432هـ،2011م ص15.

4 – ينظر:د. نوري جعفر، اللغة والفكر، مكتبة التومي، الرباط، سنة 1971م، ص106.

5 – ينظر: ابن منظور، لسان العرب مادة (أمن).

6 – 112/ النحل.

7– 154/ آل عمران.

8– 64/ يوسف.

9 – ينظر:أ.د. صالح حموش بلعيد، الأمن اللساني، أعمال الملتقى العلمي " دور التعليم والإعلام في تحقيق أمن اللغة العربية" مركز الملك عبد الله بن عبد العزيز الدولي لخدمة اللغة العربية الرياض: من14 ـــ16 / 11 / 1435 هـــ الموافق لـــ 09 ـــ11 /2014/9 م، ص 60.

10 – ينظر: أ.د.محمد علي الصامل، جهود المؤسسات الخاصة والأهلية في تحقيق أمن اللغة العربية، أعمال الملتقى العلمي " المرجع نفسه، ص 60.

11 – ينظر: أ.د. صالح بلعيد، يزع بالحاكم ما لا يزع بالعالم، دار هومة، للطباعة والنشر والتوزيع، الجزائر، سنة 2010، ص28.

12– ناصر الدين الأسد "الهُوية والعولمة" أعمال ندوة. الرباط: 1997، أعمال ندوة حول (العولمة والهوية) 27–29 ذو الحجة 1417 هـــ/ 5–7 مايو 1997، منشورات الأكاديمية الملكية المغربية، سلسلة "الدوريات" ص 62.

13– حسن حنفي "الهُوية والاغتراب في الوعي العربي" مجلة تبيّن. قطر: 2012، المركز العربي للأبحاث ودراسة السياسات، العدد 1، ص 9.

14– ينظر: محمد عادل شريح، سؤال الهوية ومتعلقاته، النظرية، الأدبيات، والإشكاليات مقال من موقع maqalwww.almultaka.net/show

15– ينظر: صالح بلعيد، هكذا رقّى الفرنسيون لغتهم، فهل نعتبر. الجزائر: 2014، منشورات مخبر الممارسات اللّغوية بتيزي–وزو.

16– الصافوط محمد، المواطنة والوطنية، ط1. المغرب: 2007، مطبعة النجاح الجديدة بالدار البيضاء، ص 71.

17- ينظر: صالح بلعيد، يزع بالحاكم ما لا يزع بالعالم، ص89.

18- ينظر: د. زهير غازي زاهد، العربية والأمن اللغوي، مؤسسة الوراق للنشر والتوزيع الأردن 2000م، ص 14.

19- عبد العلي الودغيري، اللغة والدين والهوية. المغرب: 2000، مطبعة النجاح الجديدة، ص 157.

نظام الموزع الإلكتروني في المؤسسات التعليمية

أ. بوخاتمي زهرة
جامعة جيلالي ليابس- سيدي بلعباس

الملخص: يعمل نظام الموزع الإلكتروني أو كما يسميه البعض بالحاسوب الرئيس أو الخادم أو الموفر.... على حفظ المعلومات الخاصة بمؤسسة ما، إذ لا يمكن البتة إعادة تغيير بعض البيانات والمعلومات ما دام كل المعلومات المدونة وفي جميع مكاتب المؤسسة تحفظ في الموزع الرئيسي والذي يسهر على رعايته مهندس في الإعلام الآلي، وإذا ما تبين أن هناك خطأ ما سيكون ذلك مكشوفا على الهيئة القيادية لمؤسسة، ولا جرم أن تصحيحها وتنقيحها سيكون عملا باديا للأعين.

إن الدعوة لتطبيق هذه الخطة العملية في المؤسسات الجامعية لا ينازعه بديل خاصة مع الألاعيب والتجاوزات والتزويرات التي شانت مصداقية المنتج والزبون الجامعيين على حد سواء، فلا يتسنى بذلك للبعض التلاعب بالنقاط ولا بالشهادات على سبيل الذكر وليس الحصر.

تسعى ورقتنا البحثية إلى الجوس في مسارب إشكاليات عديدة تتعلق فيما تتعلق بماهية الموزع الإلكتروني SERVEUR وكيفية عمله، وكذا المزايا التي تتبجس عن استعماله.

الكلمات المفاتيح:

الأمن المعلوماتي، الحاسوب، الحاسوب الخادم، الحاسوب الموزع، الحاسوب المركزي قاعدة البيانات، المعلومات، micro serveur ، الزبون، رسالة، طلب، إجابة، ....

المشكلة البحثية: سعيا لتحقيق الأمن المعلوماتي داخل الحرم الجامعي ودحضا للتجاوزات اللاقانونية، ينبغي البحث عن الحل الأمثل للتصدي لمثل هذه المشاكل فكان الحاسوب الخادم أحد الاقتراحات التي نقدمها، على أمل أن تكون ذات دور

فعال في تحقيق ذلك، وذات أثر إيجابي في تنظيم الإدارة الجامعية، وتحديدا لمجال بحثنا سنقتصر ونمثل بتخصص اللغة العربية وآدابها. تبعا لذلك سنحاول بحث المشكلة البحثية الآتي ذكرها: ما هي استراتيجية العمل بالحاسوب الخادم سعيا لتحقيق الأمن المعلوماتي؟

مما يفرض علينا بالضرورة الإجابة عن مجموعة من الأسئلة على رأسها:

* ما هو الحاسوب؟ ما أنواعه؟ ما هي فوائده ونقائصه؟
* ماذا عن الحاسوب الخادم؟
* كيف يتم العمل به؟ ما هي مهمته؟ وفيما تكمن أهميته؟
* ما هي فوائده وما النقائص المنجرة عن استعماله؟
* ما دوره في الإدارة الجامعية؟

المنهجية المتبعة:

تمهيد

أولا/ الأمن المعلوماتي

ثانيا/ الحاسوب: المفهوم والأنواع.

ثالثا/ الحاسوب الخادم.

رابعا/ استخدام الحاسوب الخادم في الإدارة الجامعية:

خاتمة.

المنهج المستخدم:

تفرض علينا طبيعة الموضوع أن نلجأ إلى استخدام منهج وصفي، لأننا بغرض تعريف الحاسوب الخادم، بحث كيفية استعماله وتعداد مزاياه ونقائصه.

تمهيد: بالنظر إلى التطور الفاضح والمهيمن للمعلومات، ظهرت تقنية المعلومات[1] ومعالجتها من أجل الحفاظ عليها –المعلومات– من خلال تنظيمها وحفظها وتحديثها وسرعة استرجاعها، كما وتحتاج هذه التقنية إلى نظام يعمل على حماية المعلومات المختلفة وكذا الأدوات والوسائل التي تتعامل معها أو تعالجها نخص بالذكر الحواسب الآلية.

تتعدد أجهزة الحاسوب الذي أمسى اليوم كيانا لا يمكن الاستغناء عنه، لا في المؤسسات باختلاف تنوعاتها، ولا لدى جيل الشباب، إذ تثقف معظم الآباء يبتاعون هذا الجهاز، والذي تطورت عبر السنين مهامه وتعددت فوائده، فقدانه يعني بذل الجهد الكبير في التنقيب عن المعلومات وإحصائها وحفظها، كما يعني ضياع عملية الصيانة التنظيمية للبيانات.

ومن ثم بات من الأهم على كل حصيف أن يثمّن فوائد هذا الجهاز، والأمر اللافت للنظر أن الاهتمام المتزايد به يتجلى بصورة واضحة في التطورات المتنامية، التي مست برامجه وتطبيقاته، نلمس منها الحاسوب الخادم micro serveur والذي بات بدوره لافت النظر من حيث الاستعمال في المؤسسات المنتجة، اقتصادية كانت أو سياسية أو تربوية فيما يخص الخدمات أو ....

لذا كان لزاما أن يلج المؤسسات التعليمية أخص بالذكر المؤسسات الجامعية التي طالت أيادي الهشاشة الإدارية فيها طولا مستبينا، ونحن إذ كثيرا ما نسمع عن تزوير النقاط والبيانات والمعلومات الخاصة بالطلبة وحتى بالأساتذة، ارتأينا أن مثل هذه المشقة المالية بنوعها ستنيط غبار الكثير من تلك العمليات غير القانونية عن الإدارات الجامعية، سواء وضع الخادم على مستوى الرئاسة أو العمادة حسب الإمكانيات المادية والجغرافية.

أولا/الأمن المعلوماتي: يعرف الشمري أمن المعلومات على أنه: "**اتخاذ الاحتياطات والتنظيمات التي تهدف إلى المحافظة على المعلومات في الحاسب الآلي بمأمن من الأعطال أو الحوادث أو الجرائم المتعمدة**"[2]، فأمن المعلومات

مجموعة من الإجراءات الإدارية والفنية والمصممة خصيصا من أجل حماية الأجهزة والبرامج والبيانات من السرقة أو التوقف أو التلف المتعمد أو غير المتعمد أو التخريب أو التبديل أو الاطلاع على معلومات خاصة أو الاختراقات غير القانونية...

ومن بين قضايا الأمن المعلوماتي نجد **أمن الحاسوب Sécurité du système d'information**، الذي يتضمن في جعبته بعض المهام المقتبسة عن مهام الأمن المعلوماتي، والهدف من أمن الحاسوب يتضمن: "**حماية المعلومات والممتلكات من السرقة والفساد، أو الكوارث الطبيعية، بينما يسمح للمعلومات والممتلكات أن تبقى منتجة في متناول مستخدميها المستهدفين**"[3]، وتتم عملية أمن الحاسوب من خلال مجموعة من العمليات والآليات الجماعية يصطلح عليها **بمصطلحات أمن نظام الحاسوب**، والتي تتم من خلالها حماية المعلومات والخدمات الحساسة والقيمة من النشر، والعبث بها أو الانهيار الذي تسببه الأنشطة غير المأذون بها أو الأفراد غير الجديرين بالثقة، والأحداث غير المخطط لها على التوالي[4].

مهامه: تتمثل مهام الأمن المعلوماتي حسبما ورد في تعريفه فيما يأتي:

- ✓ يضفي الشرعية على حدود وصلاحية استخدام المعلومات والأجهزة.
- ✓ يسهل الإجراءات الإدارية.
- ✓ يحمي البيانات الإدارية.
- ✓ يحافظ على المكونات المادية للحواسب الآلية.
- ✓ يحافظ على المكونات غير المادية للحواسب الآلية.
- ✓ يحمي من سرقة المعلومات أو تخريبها أو إتلافها أو اختراقها......

أهميته: تنجر أهمية الأمن المعلوماتي تبعا لأهمية المعلومات، والتي تتمثل في ضرورة الارتباط الدائم بشبكة الاتصالات والانترنيت، وعدم إمكانية عزل الشبكات المحلية عن العالمية، بالإضافة إلى اعتماد أغلب المؤسسات والمنظمات على فعالية المعلومات من حيث الحصول عليها بشكل فوري في الوقت المطلوب، ثمّ صعوبة

تحديد الأخطاء والأخطار المتربصة بالمعلومات خاصة السرية الخاصة بالمنظمات العسكرية والاقتصادية وما شابه،...

ثانيا/الحاسوب: يعرف الحاسوب على أنه جهاز يعمل إلكترونيا لإجراء عمليات منطقية دقيقة وسريعة وذلك باختزال معلومات يقدمها عند الحاجة بمعنى آخر أن الحاسوب أو الكمبيوتر وحدة وظيفية تتحكم فيها برامج مخزنة داخليا. وتمتاز هذه الوحدة الوظيفية بقدرتها على آداء حوسبية جوهرية وعمليات منطقية دون تدخل الإنسان[5].

إن هذا العمل الإلكتروني يتم من خلال إجراء العمليات الحسابية، ومعالجة البيانات بدقّة وسرعة عالية، فهو يتعامل مع آلاف البيانات الفردية الصغيرة، ويقوم بتحويلها لمعلومات أكثر فائدة بسرعة متناهية ودقة مميزة، وبإمكانه حل المسائل الرياضية المعقدة، وهناك حواسب عالية الجودة والتي تقوم بإجراء بلايين العمليات في الثانية الواحدة.

لقد تم استثمار الحاسوب في جميع الميادين من إدارات ومؤسسات تعليمية وحتى في المنازل ووو...، إذ يقدّم مجموعة من الخدمات، يعمل على تحسين مستوى الآداء، لقد أمسى ذي ضرورة ملحة، وبات الاستغناء عنه صعبا، لقد دفعنا لتغيير نظرتنا عن العالم، إذ نتمكن من الاتصال بقواعد البيانات الإلكترونية حيثما وجدت.

فالحاسوب في أبسط تعاريفه عبارة عن جهاز إلكتروني يمكن برمجته لاستقبال البيانات وتخزينها ومعالجتها ومن ثم استرجاعها.

مجالات استخدام الحاسوب:

يستخدم الحاسوب في مجالات مختلفة هي[6]:

1- ثقافة الحاسوب: يحظى هذا الفرع باهتمام متزايد في مراحل التعليم العام والجامعي حيث الغرض منه تكوين خلفية عند المتعلم عن الحاسوب وتطوره وكيفية التعامل معه ومع بعض برمجياته المختلفة.

2- **الحاسوب وسيلة مساعدة في إدارة العملية التعليمية:** ويتم التركيز في الوقت الحالي في هذا الفرع على استخدام البرمجيات التطبيقية الجاهزة مثل: معالج الكلمات وجداول البيانات في عمليات الإدارة التقليدية سواء على المستوى الإداري في المدرس في الإدارة الصفية.

3- التعليم بمساعدة الحاسوب: ويطلق عليه أيضا الحاسوب وسيلة مساعدة في التعليم، وهو عبارة عن استخدام برمجيات الحاسوب التعليمية ومختلف المواد الدراسية للتعلم الذاتي عن أو بالإضافة إلى الطرق التقليدية كالمحاضرة والكتاب المدرسي، وتقدم المادة العلمية وأنشطتها في أنماط مختلفة من البرمجيات وذلك حسب نوع المادة العلمية والهدف من البرمجية وطبيعة التعلم.

أنواع الحواسب الآلية: يمكن التمييز بين مجموعة من الحواسب الآلية:

- **الحاسب الشخصي أو حاسب المستخدم:** يعرف كذلك بالحاسوب الدقيق أو الميكروكمبيوتر أو الحاسب الصغير، يستخدم من قبل شخص أو مؤسسة صغيرة بغية تخزين البيانات، ذو قدرة محدودة على المعالجة نسبيا، يعد هذا الجهاز أحادي الاستخدام والمهام، إذ ينبغي أن يشغل من قبل شخص، نجد من الحواسب الشخصية الحاسب المكتبي والحاسب المحمول، والحاسب المنزلي والحاسب المساعد ....[7]

❖ **الحاسب المكتبي:**



يعد شخصيا يعمل على تخزين المعلومات الخاصة بالمكاتب كالنصوص والرسائل.

❖ **الحاسب المحمول:** سمي كذلك لخفة وزنه وسهولة حمله، وكذا لاندماج شاشة العرض ولوحة المفاتيح، يحتوي على بطارية قابلة للشحن، وله القدرة على المعالجة والتخزين والاستخدام.



❖ **الحاسب المنزلي:** إلى جانب شاشة الحاسوب يمكن الربط كذلك بين الوحدة المركزية والتلفزيون كشاشة عرض كبيرة.





❖ **الحاسب المساعد:** وهو نتاج التطور الكبير الذي شهدته المنظومة الإلكترونية، له شاشة عرض ولوحة مفاتيح، يسجل ويخزن المعلومات، يحمل دليل الهاتف الشخصي والتقويم وجدول المواعيد، يستعمل كآلة حاسبة، كما ويستخدم برمجيات الحاسب الآلي نفسها، فقد أمسى يسير الاستعمال مما جعله الأكثر اسخداما في يومنا هذا.

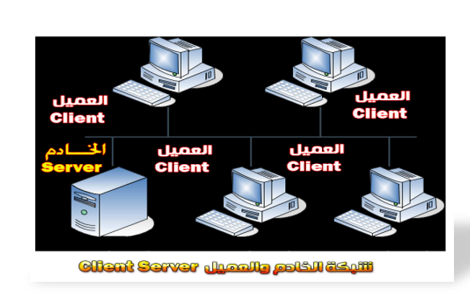
حاسب محطة العمل:



يشبه إلى حد ما الحاسب الشخصي، لكنه يتفوق عليه قدرته الكبيرة على المعالجة، وإمكانية تعدد المهام، يستخدم من قبل فرد واحد، من أمثلته الحواسب المستعملة من قبل المهندسين والعلماء في المعامل ومراكز البحوث وحتى في تشغيل المصانع[8].

الحاسب الخادم:





يتمتع هذا الحاسب بقدرات تفوق قدرات الحاسب الشخصي بعدة أضعاف عبارة عن جهاز الحاسب المستخدم من قبل المؤسسات والهيئات المتوسطة الحجم ويسمح بتعدد المستخدمين للجهاز والمستخدمين في الوقت نفسه إذ يتراوح عدد المستخدمين من 10 إلى 200 مستخدم[9]. يقومون بتشغيل برمجياتهم في وقت واحد على الجهاز.

الحاسب المركزي:





يطلق عيه اسم الحاسب الكبير لتميزه بقدرة جد كبيرة على المعالجة والتخزين فهو عبارة عن جهاز الحاسب المستخدم من قبل المؤسسات الضخمة كالشركات والحكومات الكبيرة، وما يميز هذه الحواسب قدرتها على تخزين ومعالجة كمية هائلة من البيانات وكذلك إمكانية تعدد المستخدمين وتعدد المهام، يزيد عدد المستخدمين عن 1000 مستخدم، حيث يتم ربطهم بالحاسب المركزي من أمثلته الحاسب المركزي المستخدم في الأحوال المدنية وفي البنوك الكبيرة ودار البريد المركزية...[10].

الكمبيوتر المركزي أو المتحكم في بيئة شبكاتية، يزود باقي الحواسب الآلية بخدمات تستطيع الوصول إليها عبر الشبكة، فهو نظام كبير يمكن الوصول إليه من الأنترنيت[11].

حاسبات التحكم:



يتم استخدام هذا النوع من الحواسب الآلية لإنجاز مهام خاصة كعمليات التحكم والمراقبة للأجهزة المختلفة كالأجهزة الصناعية والطبية أو وسائل النقل كالطائرات والسيارات...[12].

ويكمن الفرق بين هذه الحواسب من حيث التركيبة الإلكترونية أن صندوق المعالجة يكون أكبر في الحاسوب المركزي ثم الحاسوب الخادم بالنسبة للحاسوب الشخصي، ويتمثل الكبر في كثرة عدد الذاكرات.

الوسائط المتعددة: تعرف الوسائط المتعددة على أنها التكامل بين أكثر من وسيلة واحدة تكمل كل منها الأخرى عند العرض والتدريس... ومن أمثلة ذلك (المطبوعات، الفيديو، الشرائح، التسجيلات الصوتية، الكمبيوتر، الشفافيات، الأفلام بأنواعها)[13].

إن استخدام الوسائط المتعددة في العملية التعليمية يساعد المتعلم على إعطائه درجة كبيرة من الحرية في التعامل مع المادة التعليمية وبالتالي يكون هناك تفاعل

بين المتعلم والمادة، إذ تقدم المادة التعليمية المراد تعلمها بصورة شيقة وأكثر عمقا لذا فالمعلم منسق لاستخدام عناصر الوسائط المتعددة بحيث لا نستخدم كل عنصر بصورة منفصلة[14].

ثالثا/الحاسوب الخادم micro serveur: ضمن حواسب متعددة لشبكة واحدة نستطيع إعداد حاسوب واحد كخادم، مسؤول عن إرسال المعلومات للحواسب الأخرى والتي هي بمثابة زبائن. لقد تقمص الخادم تسميات متعددة نابعة من الوظائف التي يقوم بها، فبالإضافة إلى مصطلح الخادم نثقف عدّة تسميات الرئيسي، الموزع والموفر، مقدّم الخدمات، المضيف ....، وهناك كم يصطلح عليه بالحاسب المركزي كونه تقوم عليه شبكة الحواسب الزبائن التي تتعامل معه، بينما يتمركز الخادم بينها، إلاّ أن الحاسب المركزي شيء آخر، فهو أكبر مما يكون من الحاسب الخادم، وسيأتي توضيح لذلك.

الحاسوب الخادم عبارة عن "**جهاز يفتح للمستخدمين لتوفير الخدمات لهم كنقل الملفات وغيرها.....، الشخص الذي يدخل على serveur يسمى client**"[15]، يقوم الحاسوب الخادم بتقديم المعلومات إلى مجموعة من الزبائن قصد معالجتها أو الاطلاع عليها، كما ويقترن بهم عبر شبكة الأنترنيت أو من خلال شبكة اتصالية سلكية ما يعرف بـــ "الكابلات".

أما عن المعلومات فيتم إدراجها وتخـــزينها فيما يسمى **بقاعدة البيانات base de données /database** وهي عبارة عن "**مجموعة من عناصر البيانات المنطقية المرتبطة مع بعضها البعض بعلاقة رياضية، وتتكون قاعدة البيانات من جدول واحد أو أكثر من جدول، ويتكون الجدول من سجل (record) أو أكثر من سجل ويتكون السجل من حقل (Field) أو أكثر من حقل ومثال على السجل: السجل الخاص بموظف معين يتكون من عدة حقول مثل رقم الموظف –اسم الموظف– درجة الموظف – تاريخ التعيين – الراتب – والقسم التابع له،...الخ من بيانات الموظف تخزن في جهاز الحاسوب على نحو منظم، حيث يقوم برنامج (حاسوب)**

يسمى محرك قاعدة البيانات بتسهيل التعامل معها والبحث ضمن هذه البيانات وتمكين المستخدم من الإضافة والتعديل عليها..."[16]، يتبدى من خلال ذلك أن قاعدة البيانات الجزء الأكثر أهمية في تركيبة الحاسب الخادم بما أنها الحاملة للمعلومات.

وهناك من يجعل الحاسوب المركزي غير الخادم، فالحاسب الشخصي يستخدم من قبل الأفراد والمؤسسات الصغيرة، أما الخادم أو ما يصطلح عليه بحاسب محطة العمل يستخدم من قبل العلماء والمهندسين في الشركات والمصانع المتوسطة وقدرته على المعالجة متوسطة، فهو أقل حجما من الحاسب المركزي، وأقل تكلفة منه.

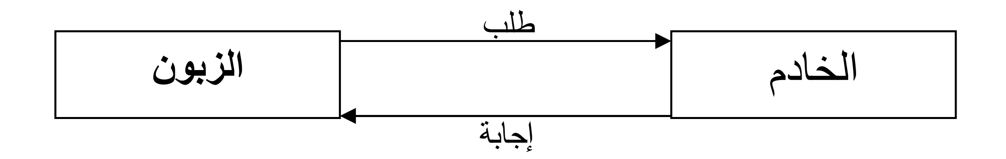
أهميته: ضمن حواسب متعددة لشبكة واحدة نستطيع إعداد حاسوب واحد كخادم، وهو المسؤول عن إرسال المعلومات للحواسب الأخرى، والتي هي بمثابة زبائن تقوم باستعمال المعلومات التي يرسلها لها الحاسوب الخادم، لذا وجب أن يكون هذا الأخير الأكثر قدرة إلكترونية، فهو ذو قاعدة بيانات، له دور تخزين وتنظيم عدد هائل من المعلومات لحساب الحواسب الأخرى.[17]

مهمته: الحاسوب الخادم كما سبق الذكر عبارة عن برمجية logiciel والتي تقدم خدمات محددة في شبكة الانترنيت، وهي الخدمات التي تنقل إلى الزبون client في شكل رسائل messages إلكترونية[18].

يشرف على الزبون ما نسميه بالعميل Agent والذي يعرف على أنه: "في نظام العميل /الموفر (client/ serveur) ذلك الجزء من النظام الذي ينفذ عملية إعداد وتبادل المعلومات"[19].

كيفية العمل به:

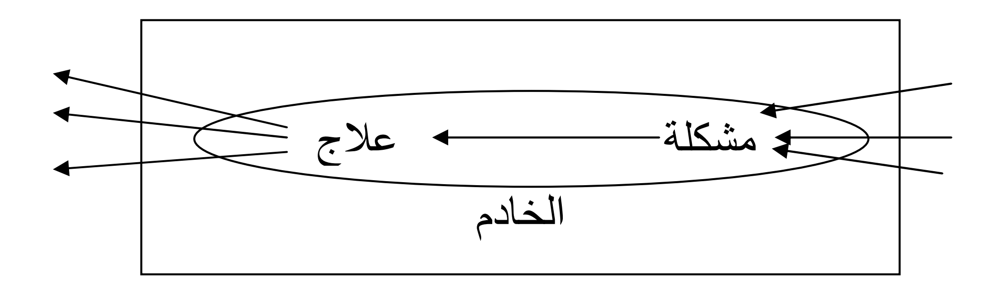
وعن كيفية عمل الحاسوب الخادم إليك المخطط الآتي:



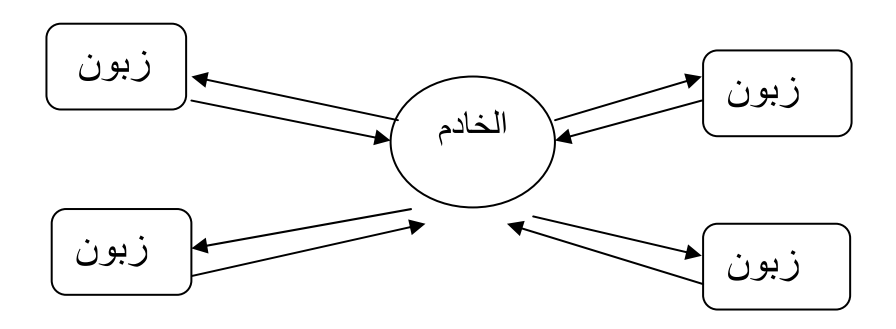
شكل 1/ مخطط يمثل كيفية عمل الخادم[20]: يتلقى الخادم رسائل طلبية من الزبون، ثم يقوم بإرسال الإجابة له. إليك التوضيح أكثر عن مفاهيم العناصر المدرجة في الشكل:

- **الزبون client**: برنامج يطلب تحقيق عملية من برنامج آخر، إذ يتضمن هذا الأخير وصف كيفية إجراء العملية المنتظر تحقيقها في شكل إجابة ضمن رسالة يرسلها الخادم.
- **الخادم serveur**: برنامج ينجز العملية المطلوبة منه من طرف الزبون ويحولها إلى نتيجة.
- **الطلب requête**: رسالة محولة من قبل الزبون إلى الخادم تصف عملية يراد تحقيقها لحساب الزبون.
- **الإجابة réponse**: رسالة محولة من قبل الخادم إلى الزبون تبعا لتحقيق العملية، تتضمن تلك الرسالة إجابة عن العملية.

إن الرسالة الطلبية تكون على شكل مشكلة يطلب من الخادم علاجها، فيقوم هذا الأخير بعمله وإيجاد العلاج أو الحل حسبما تتطلبه الرسالة الطلبية من الحاجة إلى بعض البيانات أو حل مشكلة معقدة.....



شكل 1/مخطط يبين كيفية عمل الخادم[21]: ما قد أدرجناه سابقا حول عمل الخادم يتعلق فيما يتعلق بزبون واحد، لكن للخادم شبكة تقرنه بالعديد من الزبائن إذ يتكفل كل زبون بمجال عملي محدد.



شكل 1/ مخطط يبين شبكة الخادم الإلكترونية: نلاحظ من خلال الرسم أعلاه إن شبكة عمل الخادم تتضمن مجموعة من الزبائن، لكل زبون عمليات مرتبطة بالخادم فيما يخص إرسال الرسائل الطلبية وتلقي الإجابات، كما يجدر الذكر أن الحاسوب الخادم بإمكانه أن يجري عمليات مع كل زبائنه في وقت واحد.

ملاحظة: تنبغي دوما صيانة الحاسوب الخادم بما أنه يشغل بدون انقطاع أو على مدى ساعات كثيرة نظرا لحاجة الزبائن للمعلومات الموجودة فيه، تنبغي حمايته معزولا في جهة خاصة به معزولة بدورها ومغلقة، كما يستوجب دوما الاحتفاظ بالمعلومات المخزنة فيه بطريقة أخرى كالحوسبة السحابية أو في وسائط متعددة، أو حتى إيصاله بحاسوب خادم ثان يحمل البيانات ذاتها، فإذا ما طرأ أي تلف على الخادم، كانت المعلومات مصونة في جهة ثانية.

كما يجب أمن غرفة الحاسب، من حيث إبقائها مغلقة باستمرار وعدم دخولها إلا من قبل المصرح لهم، ضرورة وضع كاميرات للمراقبة وأجهزة إنذار، وتأمينها بتقليل النوافذ والأبواب.

إيجابياته:

- سهولة التحكم ومراقبة المعلومات.
- تسيير وحدات المستعملين اثر تنظيم عملية تسهيل المرور إلى العمليات الحاسوبية.
- سمي الخادم بالمركزي لأنه يتموقع وسط الشبكة réseau ويعم على إدارة كل ما حوله.
- تجنب وضع قاعدة بيانات في كل زبون، إذ يتم وضعها في الحاسوب الخادم.

على سبيل المثال إذا تمّ تغيير نقطة طالب ما في الخادم، تتغير عند الزبون حتى ولو استخرج الطالب كشف نقاطه من الزبون يجده منقحا. فالتغيير يتم على مستوى كل الزبائن، أما إذا قام بتغييرها على مستوى الزبون ستبقى على حالها في الخادم، إلاّ إذا سمح هذا الأخير للزبون بالتغيير من خلال أمر إلكتروني.

- لا يستطيع العميل مسيّر الزبون الدخول والاطلاع على المعلومات أو القيام بالتغيير أو التنقيح ما لم يتم السماح له، أو حصوله على كلمة المرور لبيانات الخادم.

- لا يمتلك الزبائن أهمية ضمن هذا النموذج ما دام الخادم هو المتحكم الوحيد في البيانات.
- بما أن هذه الشبكة قابلة للتطور، يمكن بكل سهولة إضافة او حذف زبون أو عدة زبائن من الشبكة دون أي تأثير أو تغيير على البيانات.

النقائص:

- يحتاج هذا النموذج إلى سيولات مالية للدعم.
- أكبر مشكل يمكنه الاعتراض لهذا النموذج هو أن هذه الشبكة بخدماتها تتوقف على الخادم.

الحاسوب الخادم في الإدارة الجامعية:

دحضا لكل التلاعبات الإدارية التي مست بل وتفشّت في قطاع التعليم العالي من تزوير في النقاط، وشهادات التخرج وغيرها، وجب إناطة اللثام عنها ومحاولة التصدي لها عن طريق ضبط المعلومات والبيانات وصيانتها بشكل يحول دون العودة إليها واختراقها أو تغييرها أو تبديلها أو بأي شكل آخر غير قانوني.

فبالإضافة إلى البرمجيات الخاصة، يمكن وضع الحاسب الخادم والذي يحول دون تعرض البيانات المعبأة فيه لأي تصرف غير قانوني من قبل أي شخص مهما كانت درجته العلمية أو الإدارية ما لم يتحصل على ترخيص من الجهة القائمة على استخدام الحاسب الخادم سواء كان رئيس الجامعة أو عميد كلية ما.

ينبغي وضع الحاسوب الخادم عند رئيس الجامعة أو عميد كلية ما، ويقوم على مراقبته مهندس في الإعلام الآلي ولا تتعدد عليه الأيادي، توضع فيه جميع البيانات الخاصة بالطلبة والأساتذة لكل الكليات بأقسامها، فإذا أصاب حاسوب محطة العمل لأي كلية من الكليات أو الحاسوب المكتبي لأي قسم من الأقسام بعطب أو خلل يتمكن العميل من الرجوع إلى الحاسوب الخادم واسترجاع البيانات الضائعة.

نلمس من خلال استخدام الخادم في الإدارة الجامعية صيانة المعلومات في حالة وجود خلل أو عطب ما، سهولة استرجاعها، وكذا حمايتها من أيدي المتصرفين غير القانونيين.

الهوامش:

1- عبارة عن "تغذية ومعالجة وتخزين، ثم بث واستخدام المعلومات الرقمية والنصية والمصورة والصوتية عن طريق تقنيات الحاسب الآلي والاتصالات" الزهراني راشد بن سعيد: تقنية المعلومات بين التبني والابتكار، شركة مطابع نجد التجارية، 2004، ص35، منقول عن منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة ماجستير، قسم العلوم الإدارية، جا نايف العربية للعلوم الأمنية، السعودية، 2008م، ص17.

2- الشمري توفيق: أمن المعلومات، المديرية العامة لكلية الملك فهد الأمنية والمعاهد،1991م ص10، منقول عن منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها ص18.

3- حصاد زقاي وآخرون: معجم مصطلحات التعليم الإلكتروني، المركز الوطني للوثائق التربوية، الجزائر، 2001، ص120.

4- ينظر م ن، ص ن.

5- ينظر محمود إبراقن: المبرق، قاموس موسوعي للإعلام والاتصال، منشورات المجلس الأعلى للغة العربية، الجزائر، 2004، ص 489.

6- عبد الله سالم المناعي: الكمبيوتر وسيلة مساعدة في العملية التعليمية، حولية كلية التربية، ع 09، جا كلية التربية، قطر، 1992، ص 141.

7 -www.startimes.com

8 - www.computr03.com

9- الموقع نفسه.

10- الموقع نفسه.

11 م ن ، ص53.

12 - voir http://7aseb1.wordpress.com

12- ينظر المنظمات العربية للتربية والثقافة والعلوم :قائمة مصطلحات تكنولوجيا التربية، إدارة تقنيات التربية، تر حسين حمدي الطوبجي، 1994،ص144.

13- ينظر: جابر عبد الحميد جابر: التعليم والتكنولوجيا، دار النهضة العربية، 1983، ط2 ص235.

15- حصاد رقاي وآخرون: معجم مصطلحات التعليم الإلكتروني، ص120.

16- حصاد زقاي: معجم مصطلحات التعليم الإلكتروني، ص15.

17 - voir Oliviet Aubert : le modèle client- serveur http://www.info.uqam.ca/~obaid/INF4481/A01/Plan.htm

18- محمود إبراقن: المبرق قاموس موسوعي للإعلام والاتصال، المجلس الأعلى للغة العربية الجزائر، 2004، ص631.

19- حصاد زقاي: المرجع السابق، ص09.

20 – Oliviet Aubert : le modèle client- serveur, http://www.info.uqam.ca/-obaid/info4481/A01/plan.htm

21 - Alexandre Pauchet : informatique répartie architectures client-serveur, INSA Rouen departement ASI. p09.

دَورُ الأمن المعلوماتي في حِماية البحوث والدّراسَاتِ العِلمية

د. فاطمة صغير

<u>أوّلاً: تَمهيد:</u> شَهِدَ **العصرُ الحَدِيث**، العديدَ من التّغيّراتِ التي مسّت جميعَ جَوانب الحَياة،في مجالاتها الحيويّة فكان أن ظهرت **أنظمَة سياسيّة** وأخرى **اقتصاديّة** جديدة،فرضتها الدّول المتطوّرة؛ لتظلّ لها الصّدارة عالمياً.

ولعلّ أكثرَ التّغيّرات المميّزة لعصرنا، **الثّورة المعلوماتيّة**؛ ولذلك صار يُعرَفُ **بعصر المعلوماتيّة**؛ لِما شكّلته **المعلومات** من أهمّيّة وفائدة لكلّ دول المَعمُورة ومن ثمّ سُخّرت في سَبيل انتقالها كلّ الوسَائل والسّبلِ **كالأثير والكابلات البَحريّة والبرّيّةِ**، كما اهتَدى العَقل البَشرِيّ إلى **أجهزَة إلكترونيّة** جديدة وفَريدَة، سَاعدَت على بُروزِ سَيل عارمٍ من **المَعلومات**، مثلما هو الشّأن بالنّسبَة **لجهاز الحاسوب أو الكومبيوتر.**

لقَد غدا **الحَاسُوب** ضرورَة قُصوى، فسَجّل انتشَارا واسِعاً،داخِل المؤسّساتِ والإداراتِ؛ نظرا للخَدمَات الجليلة التي يوفّرها، ومن ثَمّ لم يعد الفردُ قَادرًا على إنجَاز أعمَاله ومشَاريعه، دون استخدامه، وما كثرة **المقاهي** وتزايُدها يومًا بعد يومٍ إلاّ دَليل قَاطع على ما صَار يُشكّله **الحاسوب** في حياتنا اليومِيّة.

والحَديث عن **الحَاسُوب** ومختلف الخَدمَات التي يوفّرها، لا يَكتَملُ إلاّ بالكَلامِ عن أهمّ تلك الخَدمَات، ونَقصد بذلك خِدمة **الإنترنت.**

لقَد أضحَت **شبكَة الإنترنت** عَاملاً أساسيًا وحيويّا في حَياة الكَثير منَ النّاسِ حتّى صارَ الجيلُ الجديد، يُعرف بتسميّة **الجيل الرّقمي** الذي استَهوته هذه الشّبكة وأصبَحت لديه من أهمّ أدوات خلق **التّفاعل التّكاملي وتطويره**، خاصّة حين وفّرت له أسهَل الطّرق؛ لإرسال واستِقبَال مختَلف **المَعلومَات**، عن طريق ما يُعرَف

بالبريد الإلكترونيّ الذي سَاعد الأفرادَ على التّواصُل والعمل المشتَرك، بشَكل مريحٍ، لدرَجة أن أصبَح العَالم كلّه قريَة صَغيرة تحت أيدينَا.

وتشير آخر الإحصائيات إلى أنّ مستَخدمي **شَبكَة الإنترنت،** في تَزايد مستمر سواء داخل **الدّول الأجنبيّة أو في البلدان العَربيّة** التي تجاوز فيها عدد مستَخدِمي الشّبَكة **ثمانية وثلاثين مليون** مستَخدم، وسجّلت **دولة الإمارات** وحدَها أعلى معدّل للانتشَار، تَليهَا دَولة **قَطر، فمَملكة البَحرَين ومصر.**[1]

والوَاقع أنّ **شَبكات الإنترنت،** اتّسع مجَال استِخدامها كَثيرًا، فَهي مُعتمدَة بشَكل مُطلقٍ في كلّ مَجَالات الحيَاة: **السّياسية والاقتصَاديّة والتّجاريّة والعلميّة** إذ تُسَاعد على العَمل بِسرعة ودونَ وسطاء، ومن دون استِخدام قَنوات الاتّصال التّقليديّة، كما وفّرت إمكانيات مُتسَاوية للجَميع وفي كلّ أنحَاء العَالم، فَسهُلت الحَياة، وتوفّرت **الخَدمات** بكَيفية يسيرَة وسَريعة، حتى غدا الفَرد المسافِر بإمكانه حَجز وسيلَة السّفَر والإقَامة، قَبلَ أن يَبرَح محلّه، وأيضا صَار بمَقدورِه التّسوق والتّعرّف على مُختَلف السّلع والبَضَائع، ثمّ الاقتناء إذا أرادَ، وكلّ ذلك في ظَرف دَقائق معدودة.[2]

غَير أنّه لاَ يُمكن الانبهَار بمَا يُقدّمه **التّطور التّكنولوجي للمعلوماتيّة،** فَبقَدرمَا يُوفّر للإنسانيّة من خدَمَات جَليلة ونَوعيّة، فَإنّه بالمقَابل حَملَ إليها منَ **المَخَاطر والمخَاوف** ما قَد يَجعَل **التّقنية المعلوماتية،** في زاوية من زَوايا النّسيان والخَوف والإهمَال، ومن ذلك أنّ التّزايد المستمر لمستخدمي **الشّبكة العنكبوتية،** انجرّ عنه وجود **مُهاجمين ومتطفّلين** صَاروا يقضون السّاعات في سَبيل مُحَاولات **الاختراق أو سرقة مَوقع** من المَواقع **أو الوصُول** إلى معلومَات مُهمّة وحسّاسة، تُؤدّي بصَاحبها إلى عَمَليات **الابتزاز المادي والمَعنَوي.**

وهكذا لم يَعد يَخفى على أحد أنّ العَالم اليَوم، يُواجه الكثيرَ منَ سلبيَات **التّطوّر التّكنولوجي** للمعلومَاتية، **كالتّضليل** والزّيادَة العَاصفة **للجَرائم** المُرتَكبَة، عن طريق **الحَاسبات الإلكترونيّة،** وخاصّة في المَجالات **الاقتِصَاديّة والمَالية؛** إذ تشيرا لدّراسات في هذا المَجال إلى أنّ العَديد من **المُجرمين،** تَمكّنوا من الوصولِ إلى

معلومَات سرّيّة وقَاموا **بنَسخها وإجراء تَعديلات** عَلَيها، وفي الكَثير منَ الأحيان يَقومون **بإتلافها**، وبسبب هذه التّجَاوزات والاختِراقَات تضرّرت العَديد منَ الشَركَات في العَالم، ممَّا اضطرّها إلى التّفكير في سُبل **الرّدع والحِمَاية.**

وأمَامَ الخَسائر الفَادحَة التي لَحِقت **الشّركات العَالميّة**، جَرّاء **جَرائم الحَاسبات الالكترونيّة**، قَامت عَدد من الدّول المُتقَدّمة **كالولايات المُتحدة واليابان وألمانيا وإيطاليا وروسيا وفرنسا وكندا وبريطانيا** بإعداد خطط لمُكافحة **الجَريمَة الالكترونيّة.**

ومنَ **التّدابير** التي اتّخذتها هذه الدّول: إدخَال عَدد كاف منَ المُتَخصّصين القَادرين على تَوفير التّعَاون التّقَني في مَجال المُكافَحة.

ولاَ يَزال هاجِس توفيرا **لأمن للمَعلومات**، يُقلق بَال الكثير من المستفيدين منَ **التّطوّر التّكنولوجي للمَعلومَاتيّة** حتّى عمّ مصطلح **أمن المَعلومات** information security فمَا المُراد به؟

<u>**ثانياً**</u>**:** <u>**مفهوم الأمن المعلومَاتيّ**</u>: بعدَ شُيوع مُصطَلح **أمن المَعلومَات**، تَلَقفه العَديد منَ البَاحثين بِهَدف تَحديد مَفهومِه ودلالَته؛ ولذلك نُصَادف الكَثير منَ المَفاهيم أشهَرها:

1- هو مَجموعَة منَ الإجراءات والتّدابير الوقَائية التي تُستَخدَم، سَواء في المَجال التّقني أو الوقَائي؛ للحفَاظ على المَعلومَات والأجهزة والبَرمَجيات إضَافة إلى الإجرَاءات المُتَعلّقَة بالحِفاظ على العَاملينَ في هذا المَجال.[3]

2- إنّه الحِفَاظ على المَعلومَات المُتَواجدة في أيّ فَضاء مَعلومَاتي، منَ مَخَاطر الضّيَاع والتّلف أو من مَخَاطر الاستِخدام غير الصّحيح، سَواء المُتعمّد أو العَفوي أو مَخَاطر الكَوارث الطّبيعيّة.

3- يُمثّل مَجموعة التّدابير الوقَائية المُستَخدمة في المَجالَين: الإداري والفَنّي؛ لِحمَاية مَصَادر البَيانَات من أجهزَة وبَرمَجيات وبَيانات من التّجَاوزات أو

التَّداخُلات غير المَشروعَة التي تَقَع عن طَريق الصُّدفة أو عَمدا عن طَريق التّسلّل.[4]

من خلال هذه المفَاهيم، يُمكِنُنا الوصول إلى أنّ **أمن المَعلومَات،** حَقل جديد عَرفَه **عَالم المَعلومَاتيّة،** يَهتمّ بدِراسَة طرق **حِماية البيَانات المُخزّنة في أجهزة الحاسُوب،** بهَدف التّصدّي للمُحَاولات الرّاميّة إلى الدّخول غير المَشروع إلى قَواعد البَيانات مَخافة **تَغييرها** أو **تَخزينها.**[5]

<u>**ثالثا: البُحوث والدّرَاسَات العلميّة على شَبَكة الإنتَرنت:**</u> **الإنترنت** وسيلَة عِلمِيّة إعلاميّة، فاقَ حُضورها في حَياتِنا اليَوميّة أنواع **الميديا** الأخرى؛ لِمَا تَتَميّزبه عن غَيرِها من وَسَائل **التّطوّر التكنولوجي، كالسُّرعة** في تَقديم المَعلومَة والحِرص على **تَنوعِها،** فَهي تَحتَوي خَزينا كَبيرًا وهامّا من **المَعلومات** في **مُختَلف التّخَصّصات والفُروع العلميّة** كَما تُوفّر العَديد من الخَدمات للطّلبَة والباحثينَ **كَدليل الجَامعَات ودليل البَاحثين ودَليل المَجلّات؛** ولذلك أقبلَ **أهل البُحوث والدّرَاسات العلمِيّة** عَلى هذه التّقنيّة باعتِبَارها **وسيلَة اتّصال وتَواصل،** مَكّنتهم من **إرسال الرّسَائل** وسَمَحت لَهم **بمُحَاورة** غَيرهم، بِهَدف **الإطلاع على أفكَار وآراء بَعضهم البَعض.**[6]

وليسَ هذا فحَسب وإنّما سَاعَدت **شَبكَة الإنتَرنت** مُختَلَف البَاحثين أسَاتذة وطَلبة عَلى **ارتياد المَكتَبات** من خلال **تَسهيل عَمليّة الإعَارة** والوصُول إلى مُختَلف **الأبحَاث والدّراسَات.**

لقد ارتَبط **البَحث العِلميّ** إذن **بشَبَكة الإنترنت،** ارتِبَاطا وثيقًا، ولم يَعد من المُمكِن تَصوّر قِيام **البُحوث والدّرَاسات** بَعيدا عَنها، بِدليل ذلك الكمّ الهائل من **الإنتَاج العِلمي والفِكري** الذي نَجده على صَفَحات العَديد من **المَواقع** حيث نُشِر بهدف إفَادة أهل العِلم والمَعرفة من جهة والتّعريف بذلك الإنتَاج من جهة أخرى.

وهكذا لم تَعد **تقنيّة الإنترنت** فقط مُستَودعا **للمعلومَات** الخَاصّة بالمَجال **الاقتِصَادي والمَالي والتّجَاري والعسكَري،** وإنّما هي أيضًا **بنك مَعلومَات** في المَجال **الفكري والعِلمي والثّقَافي.**

فالمتَجوّل عبرَ صَفَحَات مُختَلف **المَواقع ومُحركّات البحث**، يَجد الكَثير من البَاحثين والدّارسين قَد اعتَمَدوا **شبكَة الإنترنت**، يعرضون من خِلالها مَا أعدّوه من **مَقَالات ودِراسَات وأبحَاث**؛ وذلك بشتّى الكيفيات حَيث نَرى البَعض منهم يَنتَسب إلى **منتَدى** من المُنتَديَات، يَعرض عن طريقه **أعمَاله العلميّة** أو يُخوّل **لمَركَز** من مَراكِز البَحث مَهمّة **التّعريف بإنتاجه العِلميّ**، ولربّما فضّل البَعض الآخر اتّخَاذ موقع الكتروني به، يكفُل له هذا الأمر.

والجدير بالذّكر أنّ **شَبكَة الإنترنت**، حظيت بالعديد من **المُنتَديات والمَراكز العِلميّة**، على نحو **منتَديات المَنشَاوي للدّراسات والبُحوث**،[7] فهذا المَوقع يَضمّ العديد من الأقسام التي تَسهر على:

أ. **التّسهيل على البَاحثين والطّلبة الاستِفَادة من البُحوث والدّراسَات المنشورة.**

ب. **نشر المَقالات والمُقابلات الصّحفيّة التي تنشُرها وَسائل الإعلام بشَأن مُشَاركات البَاحثين وكذلك البحوث التي يَقومُون بها.**

ج. **تَوضيح عنَاوين البُحوث والدّرَاسَات الجَديدة التي تنجز حديثًا.**

د. **نشر المُؤتمَرات والنّدوات، بهَدف حثّ البَاحثين وطلبة العِلم على المُشاركة فيها.**

ه. **نشر الكُتب الإلكترونيّة المُختَلفة.**

ومن المَراكز العِلميّة المُهتَمّة **بالبُحوث والدّراسَات**، نجد **مركز الملك فَيصل للبُحوث والدّراسَات الإسلاميّة**[8] والذي يلعب دَورًا هَامّا في تطوير **الحياة العلمية والمَعرفيّة** كَما يَعمل على تَحفيز الطّاقات المُبدِعة في المُجتَمع، مُسَهلاً مهمّة البَاحثين والدّارسين في الوصول إلى **المَعلومات**.

ومثل هذه المَراكز والمُنتَدَيات في الجزائر، نجد **منتَدى الجَلفة** المَشهور بنَشاطه المُتَنوّع؛ إذ يُعرّفنا بمُختَلف **الأبحاث والدّراسات** المُعدّة من قِبل البَاحثين المُتَخصّصين، كما يُطلعهم على **النّدوات والمُؤتَمرات العِلميّة** التي تُنظمُها مُختلف الجامعات داخل الوطن وخَارجه.

والحَقيقة أنّ **مَراكز البُحوث والدّراسَات**، تُمثّل إنتَاجا ثَقَافيا وحضاريا مُتَميّزا؛ لأنّها مرآة تَعكس اهتِمَام المجتَمع بالعِلم والمَعرفة، كما تَعكس توجّه المُجتَمع في حفظ تُراثه ومُنجَزاته المَعرفيّة والعِلميّة والحضاريّة؛ ولذلك صَارت هذه **المَراكز والمُنتَدَيات** ضرورة حضاريّة لا يَستَغني عنها أيّ مُجتَمع من المُجتَمعات.

ولأهمّيتها بالنّسبة **للبَاحثين وطَلَبة العِلم**، رَاح المُشرفون على هذه المَراكز يَتّخذون لها **مَواقع** تَخصّها كما عَملوا على تَطويرها عن طريق صَفَحَات تُعبّر عَنها وتُقدّم من خلالها مختَلف الخدمات، بُغية تَزويد أهل العِلم **بالمعلومة** الجَديدة والموثّقة.

<u>رابعاً: مَوقف الأكاديميين من البحوث والدّراسات العلميّة على شبكة الإنترنت</u>

إنّ اعتِمَاد **الدّرَاسَات والبُحوث العِلمِيّة** المَنشورة على **صَفَحَات مَواقع شَبَكة الإنتَرنت**، لم يَسلم من الانتِقَاد أو على الأقلّ من التّحفظ؛ ذلك لأنّ الكَثير من أهل العِلم والبَحث، لا يَثقون فيمَا يُعرَض على الشّبكة من دراسات لعدّة أسباب منها:[9]

أ. **غِيَاب الدّرَاسَات ذات المَعلومَة المُهمّة والقيّمَة؛ لأنّها لا تُتَاح مَجّاناً على الشَبَكة، وإنّمَا هيَ ذات تَكاليف باهظة.**

ب. **غِيَاب الرّقَابة على ما يُنشَر على الشّبكة؛ إذ يُمكن لكلّ من أرَاد أن يَنشُرَ دونَ أن يَخضع العمل المَنشور للتّقويم.**

ج. **غياب التّهميش والتّوثيق فيما يُنشَر من أعمال علميّة؛ بسبَب استخدام تِقنِيَات سَيّئة لا تفي بِمُتَطلَبات إظهار الإيضاحَات، الأمر الذي يَضرّ بالنَاحيّة الشّكليّة والمَنهَجيّة للإنتاج العِلميّ المنشور.**

إنّ هذه الأسباب تَخصّ مَسألة **الثّقة** فيما يُنشر وأيضاً تتَعلّق بنِسبة **جَودته** إلاّ أنّ هذا الحكم لا يُمكن تَعميمه؛ لأنّنا نَجد **دِرَاسَات علميّة رائدة**، أراد أصحابها أن تكون في متَنَاول طلَبة العِلم والمَعرفَة؛ إلاّ أنّنا لا نَعدَم تَخَوّف هؤلاء على جُهودهم العِلميّة، بسَبب **السّطو** عليها **للانتِحال والسّرقة**، ولهذا أصبَح منَ الضّروريّ اتّخاذ **الإجراءات اللاّزمة و التّدابير المنَاسبة** من أجل **حِماية البُحوث والدّرَاسات العِلميّة** المَوجودة على **شَبكة الإنترنت**، وهذا الأمر لن يتحقّق إلاّ بالعودة إلى **أمن المَعلومات** لأنّه من المُفيد والنّافع أن تَتَوفّر تلك **البُحوث والدّرَاسَات الأكاديمية** بشكل مُريح، ولكن إلى جانب ذلك لا بدّ من **بَرنَامج دقَيق**، يَكفُل أسَاليب **حِمَاية الإنتاج العِلميّ من التّشويه والسّرقَة** وفي ذات الوقت يَضمَن **حُقوق أصحَابه**، وهذا الذي يَعمَل عليه **بَرنَامج أمن المَعلومَات.**

<u>خامساً</u>: <u>الأخطار التي تُواجه البحوث والدّرَاسَات العِلميّة على شَبَكة الإنترنت</u>

باتَ أكيدًا لدينا أنّ **شَبكة الإنترنت** أداة مهمّة **للبَحث العِلميّ**، وأمَام طبيعة الخَدمَات التي تُوفّرها لمُستَخدِميها بشَكل سَريع، **كسُهولة الاقتبَاس وتَعديل البرمَجِيات**، أدّى إلى الإغرَاء **بسَرقة المَادّة العلميّة والسّطو عليها**، إمّا بهدف **تَحريفها أو تَخريبها أو تَشويشها أو إعَادة إنتَاجها** لأهمّيتها البالغة.

وللإشارة فإنّ مثل هذه السّلوكات البَعيدة عن الأخلاق، لم تكن منتَشرة في بداية استِعمَال **الشّبكة المَعلومَاتية** لاقتصَار استِعمَالها على الطّبقة الأكاديميّة من فئة البَاحثين وطلبَة العلم، إلاّ أنّ التّوسّع المُذهل في استِعمَالها ودخول فئات أخرى إلى قائمَة المُستَعملين والمُستفيدين، أدّى إلى ظهور تلك **التّجاوزات والأخطار.**[10]

وإذا أرَدنا مَعرفَة نَوع **الأخطار** التي توَاجِه **الإنتَاج العلميّ** علَى **شَبكة الإنترنت** فإنّنا نَحصِرها فيما يلي:[11]

أ. <u>**الفيروسَات**</u>**: الفيروسَات** من أكثَر **جَرَائم الإنتَرنت** انتِشاراً وتأثيرا؛ إذ تَتَسبّبُ في إتلاَف المَادّة المُخزّنة، وفي هَذه الحَالة تَسهُل **عملَيّة سرِقَتها واستِغلاَلِها** بطُرُق غير شَرعيّة؛ ولذلكَ يتَوجّب علَى الخُبَرَاء إعدَاد مُضَادَات لكُلّ أنوَاع الفَيروسَات بهَدَف **حِمَاية المَادّة العِلميّة.**

ب. <u>**انتحال الشّخصيّة**</u>**:** هذه **الجَريمَة** بدَورهَا من الجرَائم المُنتَشرة، وهيَ تَنَال من **حُرّية وأمن خُصوصيّة الأفرَاد والمُؤسّسَات**، ومن ثَمّ فإنّ **الدّرَاسات العِلميّة** المُنتَشرة على صفَحات المَوَاقع، قَد تُسوّل للمُجرِمينَ **انتِحَال شَخصيّة أصحَابها**، من أجل الاتّصَال بنَاشرينَ ومُؤلِفينَ **لشرَاء نُسَخ المُؤلفَات والكُتُب.**

ج. <u>**التّشويش والتّصَرّف في المَادّة العِلميّة**</u>**:** يتسنّى للمُخَرّب عن طَريق **عَمليّة الاختِراق التّشويش على المَعلومَات والبيَانات**، أثناء **عَمَليّة البثّ والاستِرجَاع.**

د. <u>**النّصبُ والاحتِيَال**</u>: قَدّمت **الإنتَرنت** فُرصَة **الإتَاحَة والتّدَاول والاتّصَال والتّواصُل** ، ممّا سَاعدَ أصحَابَ النّوَايا التّخريبيّة على **بَيع الإنتَاج العِلميّ أو نَسخِه** بِطُريقَة لا مَحدودَة ، الأمر الذي يَجعَله عُرضَة **للسّرقَة.**

إنّ هذه **الأخطَار** وغيرهَا، لا يُمكن مُجَابَهتها إلاّ عن طَريق **تَدابير وإجراءات أمن المعلومات** الذي يُساعدُ على:[12]

أ. **الحِفَاظ عَلى الإنتَاج العِلميّ وحِمَايَتِه من جَميع أشكَال الجَريمَة الإلكترونيّة.**

ب. **إتَاحَة وتَداول الأبحَاث العِلميّة عن طَريق عَمَليّة البثّ والنّشر، دونَ تَحريف أو تَحوير أو تَشويش.**

ج. **حِمَاية حُقوق المِلكيّة الفكريّة للبَاحِثين والمُبدِعينَ.**

د. **احترَام خُصُوصيّة الإنتَاج العِلمِيّ، أثناء الاستِفَادة منه والإحجام عن التّعدّي علَيها.**

ولتَحقيق هذِه الغَاية، رَاحت مُعظمُ الدّول تُشَرّع **قَوانين ونُصوص**، تَحمِي **الحُقوق والحُرّيات والخُصوصيّة**، علماً أنّ هذه الحِماية تَمسّ حقّ الكَافة في الحصول على **المَعلومة** وأيضا **حُقوق أصحاب الإبداع.**

ولأهمّية هذه **النّصوص التّشريعية**، أصدرت الجزائر عام **2003 الأمر رقم 05/03** والذي يتَعلّق بحقّ المؤلّف والحقوق المُجاورة والذي يساير في مُجملَه التّطوّرات الحَديثة الحَاصلة في ميــدان التّشريع أو التّقنيات الحديثة كَما سنّت **المَادّة 03** التي تنصّ على إدخَال برَامج الحَاسوب في إطار المُصنّفَات المَحميّة بمُوجب **حقّ المُؤلف** كما نصّت **المَادة 41** عَلى عَدم **الاستِنسَاخ الخَطّي لكِتَاب كَامل أو مُصنّف أو برَامج الحَاسوب.**

هوامش البحث:

---

1 – ينظر: الأنترنت ومبادئ الأمن المعلوماتي الدّولي، د. محمد البخاري، بحث نشر بموقع: https//ar.wikipedia.org.

2 – ينظر: الأنترنت والعولمة، بهاء شاهين، عالم الكتب، القاهرة 1999، ص: 63.

3 – ينظر: مقال أمن المعلومات، بحث نثر بموقع ويكيمكتبات الموسوعة الحرّة في علم المكتبات والأرشيف.

4 – ينظر: نظم المعلومات الإدارية، حميم نجم عبد اللّه السّامرَائي، دار وائل، عمان، 2005 ص: 223.

5 – ينظر: قواعد البيانات، قطيشات منيب، دار وائل، عمان، 2005، ص: 235 و236.

6 – ينظر: دراسة حديثة عن استخدام الأنترنت في البحث العلمي، حميد الهاشمي، منتدى اجتماعي على الرّابط:
http//www.ejlemay.com

7 – ينظر: منتديات المنشاوي للدّراسات والبحوث على الرابط http//www.minshawi.com

8 – ينظر: موقع مركز الملك فيصل للبحوث والدّراسة: دراسة تقويمية للباحثة هند بادي علي بادي، عرضتها دورة إلكترونية فصلية محكّمة ومتخصّصة

9 – ينظر: تحديث القوانين في عصر المعلومات، أعمال النّدوة العربيّة للمعلومات، زياد فداء قسنطينة 2000، ص: 61.

10 – ينظـــر: أمـــن المعلومـــات أحـــد السّبل لحمايـــة الملكيّة الفكريّة، فؤاد ضيف الله، عدد 24 ديسمبر 2010.

11 – ينظر: جرائم الأنترنت، حسين بن سعيد الغافري، http//www.inf-te.com

12 – ينظر: أخلاقيات المعلومات في مراكز المعلومات والمكتبات العربيّة، فتحي عبد الهادي محمد، ع1، 200، ص: 42، وأيضاً مثاق عربي لأخلاق مجتمع المعلومات، مجلّة النادي العربي للمعلومات، العدد 29 مارس 200" ص: 25.

إدارة
مكتبة معهد الخرطوم الدولي للغة العربية
مشروع إدارة مكتبة رقمية معلوماتية آمنة

أ.د. فهد سالم خليل الراشد
باحث لغوي من دولة الكويت
أمين مكتبة معهد الخرطوم الدولي للغة العربية
مدير تحرير المجلة العربية للدراسات اللغوية

ملخص المداخلة: تعد المكتبة عصب الحياة الثقافية والعلمية والفكرية، كما تعد المدرسة الثانية للطالب والدارس، وهي المعلم المساند، وهي الرافد المعين للباحث والمعلم والطالب معا.

ولا يختلف اثنان على أن مكتبة معهد الخرطوم الدولي للغة العربية، ثرية بمصادرها ومراجعها، زاخرة بكتبها ومؤلفاتها، غنية بدورياتها وحولياتها، ولعل الأهم من ذلك كله فهي كنز ثمين بما لديها من رسائل علمية التي يصفها مدير المعهد قائلا "تمثل الرسائل الجامعية التي تعد في المعهد بحوثا تكميلية للمقررات الدراسية التي يدرسها الطلاب في مستويات الدبلوم العالي والماجستير في اللغة العربية للناطقين بغيرها. واتجهت هذه البحوث منذ تأسيس المعهد اتجاهات متعددة أساسها اتجاهات علم اللغة الحديث بفروعه، وأهمها علم اللغة العام، وعلم اللغة التطبيقي، وعليم اللغة الاجتماعي، والنفسي، وعلم اللغة التقابلي الذي اهتم بالمقابلة بين دراسة اللغة العربية واللغات التي يتحدثها طلاب المعهد القادمين من مختلف

دول العالم.وتشكلت لدى مكتبة المعهد حصيلة ثرة ونادرة في هذه المجالات تناولت قضايا تعليم اللغة العربية، واللسانيات، والمعاجم ثنائية اللغة، وعلاقة لغات الشعوب الإسلامية باللغة العربية"[1].

كل ذلك يحتم علينا حماية مقتنيات إدارة هذه المكتبة من التلف أو السرقة المعلوماتية بتحويلها إلى إدارة مكتبة رقمية لتحقيق الأمن المعلوماتي، ولتيسير سبل الوصول إلى المعلومات والإفادة منها في الحقل اللغوي.

تمهيد: لا نبالغ إذا قلنا إن من أهم المؤسسات العلمية والتربوية المعنية بالأمن المعلوماتي هي المكتبات بكل أنواعها.

ولأن المكتبات تعد عصب الحياة الثقافية في جميع الحقول العلمية، كما تعد المدرسة الأولى من حيث توفير الكتب والمصادر والمراجع والدوريات التي تساعد على تلقي العلم والمعرفة في المدارس والمعاهد والجامعات المتخصصة، وكلما تنوعت المكتبة بمعارفها وعلومها، كلما شحذت واستثارت همم الباحثين والدارسين والمؤلفين للإبداع والابتكار؛ فعبقرية أية أمة إنما تقاس بنتاجها من العلوم والمعارف.

ولئن تعددت التسميات "كما يدور الحديث الآن بين العلماء عن تسميات جديدة للمكتبة، كالمكتبة الافتراضية virtual والمكتبة السيبرانية cibrary والحقيقة، رغم هذه التسميات فمصطلح (المكتبة library) لن نستطيع أبدا تغييره، وإذا غيرناه فسنفقد معنى المكتبة ووجودها والهدف منها؛ فمصطلح (المكتبة) لا يمكن الهروب منه، فهو مصطلح، مثل السماء والأرض والإنسان، تشبعت جذوره بكل ما في الكلمة من معنى، بثقافة العالم وموروثاته"[2].

ولئن أصبح العالم كما يقال "قرية صغيرة" بفضل التكنولوجيا الحديثة، المتمثلة بوسائل الإعلام والاتصال (المرئي والمسموع والمكتوب)؛ ففي الوقت ذاته اتسعت فضاءاته المعرفية، فوجدنا أنفسنا أمام ثقافات متعددة لمجتمعات متباينة من حيث اللغات والعادات والتقاليد، وأصبح لزاما علينا أن نعيش هذه المرحلة ونتفاعل مع معطياتها بتعريف للثقافة قد يكون بسيطا في صياغة كلماته، إلا أنه وبلا شك سوف يكسر حاجز الخوف من ثقافة الآخر، فنحن ننظر للثقافة على أنها: احترام ثقافة الآخر: ولأن الإنسانية – في نظرنا – هي إحساس وشعور بالآخر، وهي مبادئ وقيم ومثل عليا، وهي مراعاة للمواقف والظروف، وهي مشاركة وجانية في الأفراح والأتراح، وهي شفافية ومصداقية في التعامل، وهي تحنان وعطف، وهي أمل وتفاؤل، وهي تقاسم وإيثار، وهي مجموعة من الصفات التي يتحلى بها البشر؛ أردنا أن نجد وسيلة اتصال قوامها ما سلف، لكي نلبي رغبة الدول العربية والإسلامية بالمحافظة على تراثها وموروثها الإنساني والثقافي والحضاري، وبما يلبي طموح الدول العربية والإسلامية في امتطاء صهوة الحضارة العالمية المعاصرة والاستفادة منها وممازجتها مع ما لدينا من حضارة وثقافة، والمحافظة على أصالتنا، وأمل الدول العربية والإسلامية في غد مشرق يخدم الإنسانية قاطبة تحت ظل التعايش السلمي؛ فلم نجد أفضل من الكتاب وسيلة للتواصل الثقافي بين الأمم والشعوب.

ولما "كان الكتاب وسيلة الوعاء الأساسي للمعرفة"[3]؛ فلا شك بأن المكتبة حاضنة لهذا الوعاء والمحافظة له من التلف والإهمال والسرقة.

لنطرح عدة أسئلة عن مفهوم (الكتاب) الاصطلاحي في عصرنا الحالي؛ فهل يصلح (الكتاب) أن يكون بحثا أو رسالة أو مداخلة أو علما بحتا قائما بذاته أو ديوان شعر أو فكرا مستقلا ... إلخ؟

لعل من الصعوبة بمكان أن نحدد المفهوم الاصطلاحي لمعنى (الكتاب)، إذن فلنسلم جدلا بأن كل ما ذكرناه إنما هي جزئيات من مكونات الكتاب الذي لعب دورا هاما وبارزا في التقارب بين الدول والانفتاح على ثقافة الآخر، وبذلك نصل إلى نتيجة مرضية – نوعا ما – للمفهوم الاصطلاحي لــ (الكتاب) وهو (مراسل الثقافة).

ولكن كيف لنا أن نصل إلى هذا المراسل إلا بتوفير الأدوات التي يعتمد عليها الطالب والباحث من مثل (الفهارس، الببلوغرافيا، الكشافات، المستخلصات) والهم من ذلك كله إذا توفرت المكتبة الإلكترونية سوف نقوم على قاعدة بيانات للكتب يشترط فيها توحيد الاعتماد على طريقة واحدة لتوثيق المعلومات (الإلكترونية والعادية).

المقدمة

إشكالية المداخلة وجدلية المصطلح: ما بين الأمن المعلوماتي والأمن المعرفي إدارتان هما (إدارة المعرفة) و(إدارة المعلومات)؛ "فالبعض يفهم (إدارة المعرفة) على أساس كونها مصطلحا بديلا، أو مرادفا لما نطلق عليه تسمية (إدارة المعلومات)... في حين يرى آخرون أن (إدارة المعرفة) ماهي إلا بعض الجهود (المعقدة) التي تتعلق بتنظيم المداخل إلى مصادر المعلومات عبر الشبكات" "أما رجال الإدارة فينظرون إلى إدارة المعرفة على أساس كونها صرعة إدارية جديدة ليست في حقيقتها سوى جهد آخر يبذله منتجو تكنولوجيا المعلومات والاستشاريون

الإداريون لبيع حلولهم المبتكرة إلى رجال الأعمال (في العالم الغربي) المتلهفين لأية أدوات يمكن أن تساعدهم على تحقيق التقدم التنافسي الذي يبحثون عنه ويتلهفون للحصول عليه"[4].

كما يعرف بعض الباحثين (إدارة المعلومات) على أنها "حقل علمي في طريقه إلى أن يصبح أكثر شيوعا وتنظيما ويهتم هذا الفرع العلمي بضمان المداخل التي توصل إلى المعلومات، وتوفير الأمان والسرية للمعلومات، ونقل المعلومات وإيصالها إلى من يحتاجها، وخزن المعلومات واسترجاعها عند الطلب"[5].

وبهذا التعريف يتجه ظني أن (إدارة المعلومات) هي الأصل، و(إدارة المعرفة) هي الفرع، أو أن (إدارة المعلومات) قاعدة بيانات كبيرة وضخمة تضم العديد من المعارف، فإذا كانت البيانات هي أول ما يسعى إليه المكتبي – أعني بيانات الكتاب – سواء أكان مؤلفا أم مرجعا أم مصدرا أم دورية أم حولية .. إلخ؛ فلابد من إنشاء قاعدة بيانات لهذه المصنفات، هنا دخلنا في حقل المعرفة وببساطة شديدة (قاعدة بيانات) تخص المعلوماتية، أما ماهية البيانات فهي معرفية.

التعريف بمعهد الخرطوم الدولي للغة العربية: "أبرمت المنظمة العربية للتربية والثقافة والعلوم التابعة لجامعة الدول العربية في العام 1974 م اتفاقا مع دولة المقر جمهورية السودان وبدأت الدراسة في 15 / 10 / 1974 م، بمركز الخرطوم إعداد متخصصين في تعليم اللغة العربية لغير الناطقين بها. وعدل الاسم في العام 1977 م، من مركز إلى معهد الخرطوم الدولي للغة العربية.

والهدف من إنشاء هذا المعهد هو إعداد اختصاصين في مجال تعليم اللغة العربية للناطقين بغيرها، وأن يكون المتخرج فيه الكفاية العلمية في الآتي:

- تصميم النصوص متدرجة المستويات وتأليف الكتب ووضع المناهج.

- استخدام طرق التدريس المختلفة في تعليم اللغة العربية لغير الناطقين بها.
- اختبار الوسائل التعليمية وإنتاجها واستخدامها.
- تدريب المعلمين وتأهيلهم وإعدادهم للإشراف والتوجيه في مجال تعليم اللغة العربية لغير الناطقين بها.
- إجراء البحوث والدراسات العلمية.
- مباشرة الخدمات العلمية والثقافية المتصلة بالمعهد.
- استنباط طرق علمية لكتابة اللغات غير العربية بالحرف العربي.

والهيكل التنظيمي للمعهد ينقسم إلى قسمين، الهيكل الأكاديمي ويضم (مدير المعهد رئيس المجلس العلمي، والمجلس العلمي، وهيئة التدريس والشؤون العلمية وقسم نشر اللغة العربية والثقافة الإسلامية والمشروعات والبحوث.

أما الهيكل الإداري؛ فيتكون من (الشؤون المالية، الشؤون الإدارية شؤون الدارسين، قسم الخدمات والمخازن.

وللمعهد عدة وحدات منها (المكتبة – وهي موضوع الدراسة في هذه الندوة – وقسم الوسائل وتكنولوجيا التعليم، قسم الأجهزة والمعدات، ووحدة الحاسوب، وقسم مصادر التعليم).

أما البرامج الدراسية، فهناك الدبلوم العالي – الماجستير في تعليم اللغة العربية للناطقين بغيرها، البكالوريوس في تعليم اللغة العربية للناطقين بغيرها، الدبلوم العالي – الماجستير في التربية، ماجستير تخصص مناهج وطرق التدريس ماجستير تخصص الإدارة والتخطيط التربوي، ماجستير تخصص التقويم والقياس التربوي، ماجستير تخصص التوجيه التربوي والإرشاد النفسي، ماجستير تخصص تدريس اللغة العربية.

وهناك مراكز خارجية منتسبة إلى المعهد هي (معهد تدريب معلمي اللغة العربية في أثناء الخدمة في جيبوتي، قسم اللغة العربية في جامعة أديس أبابا في أثيوبيا، ثلاثة مراكز لتدريب معلمي اللغة العربية في الصومال، أربعة عشر مركزا لتعليم اللغة العربية والدراسات الإسلامية في كينيا، تعزيز اللغة العربية من خلال عدة مشروعات في تشاد، عدة برامج دراسية في جمهورية مويشيص.

إضافة إلى تعاون المعهد مع جامعات في جمهورية الصين وماليزيا)[6].

إدارة

مكتبة معهد الخرطوم الدولي للغة العربية

مشروع إدارة مكتبة رقمية معلوماتية آمنة

مدخل: تحظى مكتبة معهد الخرطوم الدولي للغة العربية بمكانة عالية ومرموقة بين الباحثين والدارسين، ولا يختلف اثنان على أن مكتبة معهد الخرطوم الدولي للغة العربية غنية بمصادر ومراجع متخصصة، وكتب هادفة، ودوريات نادرة وقيمة، ودراسات ورسائل جادة، يقصدها الكتاب والباحثون والطلاب من كل حدب وصوب على مستوى السودان وخارج السودان وكل ذلك كان وما زال بفضل العناية الفائقة التي أولتها إدارة المعهد لهذه المكتبة، كما حظي الكتاب أيضا بدعم دائم ومتواصل من المنظمة العربية للتربية والثقافة والعلوم، ومن دولة المقر جمهورية السودان؛ فهناك زيارات متواصلة من الجامعات السودانية للإطلاع على المكتبة والمعهد.

ومكتبة معهد الخرطوم الدولي للغة العربية تأتي على رأس وحدات المعهد، ثم بعد ذلك يأتي تباعا وحدة (قسم التقنيات التعليمية وحدة قسم الأجهزة والمعدات

ومختبر اللغة، ووحدة الحاسوب والآلات الراقنة)، والحق أن الوحدات الثلاثة كلها يجب أن تنضوي تحت عمل المكتبة.

يقول الباحث عبد الهادي تميم "أنشا المعهد مكتبة متخصصة وظل يزودها بالكتب والدوريات وغيرها حتى بلغت ما تضمه من الكتب (19000) بالإضافة إلى بحوث الطلاب التكميلية لنيل الدرجة العلمية والتي بلغت (1392) في مجالات اللغة العربية والتربية واللغويات والمعاجم وكتابة لغات الشعوب الإسلامية بالحرف العربي"[7].

مع ملاحظة أن ما ذكره الدكتور عبد الهادي تميم، كان في سنة 2003 م ونحن اليوم في 2015، فالمكتبة تضم (35000 ألف مجلد، بما يعادل 12000 ألف عنوان لكتاب، من غير الدوريات والحوليات والرسائل العلمية.

وفيما يتعلق بالرسائل والبحوث التكميلية التي أشار إليها الدكتور تميم في معرض حديثه عن المكتبة، يقول الأستاذ الدكتور / علي عبدالله النعيم، مدير معهد الخرطوم الدولي للغة العربية:" تمثل الرسائل الجامعية التي تعد في المعهد بحوثا تكميلية للمقررات الدراسية التي يدرسها الطلاب في مستويات الدبلوم العالي والماجستير في اللغة العربية للناطقين بغيرها. واتجهت هذه البحوث منذ تأسيس المعهد اتجاهات متعددة أساسها اتجاهات علم اللغة الحديث بفروعه، وأهمها علم اللغة العام، وعلم اللغة التطبيقي، وعليم اللغة الاجتماعي، والنفسي، وعلم اللغة التقابلي الذي اهتم بالمقابلة بين دراسة اللغة العربية واللغات التي يتحدثها طلاب المعهد القادمين من مختلف دول العالم. وتشكلت لدى مكتبة المعهد حصيلة ثرة ونادرة في هذه المجالات تناولت قضايا تعليم اللغة العربية، واللسانيات، والمعاجم ثنائية اللغة، وعلاقة لغات الشعوب الإسلامية باللغة العربية"[8].

ولما كان معهد الخرطوم الدولي للغة العربية، معهد للدراسات العليا الجامعية (ليسانس، بالكالوريس، ماجستير)، وكما مر بنا فهو معهد متخصص بتعليم اللغة العربية – ولاسيما – تعليم اللغة العربية لغير الناطقين بها، فمكتبته اكتست صفة المكتبة الجامعية، و"المكتبة الجامعية، بالمفهوم العلمي الحديث هي إحدى المؤسسات الثقافية التي تؤدي دورا علميا هاما في مجال التعليم العالي، ولا يقل هذا الدور في أهميته وضرورته عن أي دور آخر يمكن أن تقوم به أية مؤسسة علمية ثقافية وتثقيفية وتربوية وعلمية تعمل على خدمة مجتمع معين من الطلبة والأساتذة والباحثين المنتسبين إلى هذه الجامعة والكلية والمعهد"(9).

مما جعل مكتبة معهد الخرطوم الدولي للغة العربية محل اهتمام بالغ من قبل القائمين على المعهد فوضعوا لها أوليات منها:

- تزويد مكتبة المعهد بالإصدارات الحديثة وتوفير المراجع الضرورية للباحثين.
- الاستفادة مما وفرته التقنية الحديثة وتقنيات المعلومات من سبل الإطلاع على أحدث المعارف للدارسين.
- ربط المكتبة بالمؤسسات النظيرة لتبادل الفائدة.
- تحسين خدمات تقديم المعلومات للباحثين.
- تيسير استعانة الباحثين بالمراجع المتخصصة.
- الارتقاء بنوعية البحوث التي تقدم للباحثين.

الأمن المعلوماتي

مدخل: قضية الأمن بشكل عام أضحت قضية معقدة خاضعة لعد إيدلوجيات وأفكار يراها البعض متطرفة ويؤمن بها البعض الآخر، أهداف يود البعض تحقيقها

بالقوة والبعض بالحوار، وبعض يرجئها إلى وقت آخر، حقوق يراها البعض مستحقة، ويرها الآخر غير مستحقة، ومعظم ذلك إما أن يكون مكتوبا أو مضمنا في كتب متخصصة وهي في النهاية تصنف على أنها معلومات فإما أن نحفظها أو ندسها في التراب !

والسؤال هنا عن أية معلومة سوف نتحدث في بحثنا هذا؟

منذ البداية خصصنا هذه الدراسة عن المكتبات على وجه العموم وعن مكتبة معهد الخرطوم الدولي للغة العربية على وجه الخصوص. إذن نحن نتكلم عن معلومات خاصة بتعليم اللغة العربية تحتويها مكتبة معهد الخرطوم الدولي للغة العربية، كما حددنا من هم المستفيدون من هذه المعلومات؛ فبات لزاما علينا أن نؤمن هذه المعلومات من الضياع والتلف والسرقة؛ فعزمنا العقد على إنشاء مكتبة رقمية، لذا؛ يتطلب الأمر إلى إعادة هندستها، و"تتمثل عملية إعادة الهندسة في تغيير طرق عملنا، وبصفة أدق فإن تركيب أجهزة الكمبيوتر في المكتبات لا يعني إعادة هندستها للعصر الرقمي، فليست التكنولوجيا في ذاتها التي تحدد إعادة الهندسة بل كيفية استخدام التكنولوجيا كجزء من إعادة تصميم طرق العمل"[(10)].

وكلما ازدادت فرحتنا باستخدام التكنولوجيا الحديثة والمعاصرة في إدارة المكتبات لسهولة الوصول إلى المعلومة وتيسيرها بطريقة سريعة، كلما ازداد قلقنا على السطو على هذه المعلومات من قراصنة الإنترنت وأصبح لزاما علينا وضع خطة آمنة لحفظ هذه المعلومات وسلامتها والمحافظة – أيضا – على خصوصيتها وبذلك يجب أن ننطلق من عدة محاور أهمها:

1- علماء كمبيوتر.

2- أمناء مكتبات.

3- خبراء في تكنولوجيا التعليم.

4- مصممو برامج.

مواقع الإنترنت: أرى أن أفضل تعريف للإنترنت هو "مكتبة إلكترونية" يجمع بين الإدارة المعلوماتية والإدارة المعرفية، كما "تعد مواقع الإنترنت أحد المصادر الهامة في بحوث علوم المكتبات والمعلومات، وقد حظيت حديثا باهتمام كبير من جانب الباحثين المتخصصين في مجال لدراسة مختلف الجوانب المتعلقة بها من حيث: التعريف، والأهمية وطرق الاستفادة منها"(11).

والإنترنت كما يعرفها أحد الباحثين هي "شبكة فضائية ضخمة تتكون من أجهزة الحاسوب الآلي المرتبطة ببعضها البعض والمنتشرة حول العالم، حيث توفر العديد من الفرص للمستفيدين في الحصول على المعلومات التي يرغبون في الحصول عليها، كما تعتبر الإنترنت من أهم الأدوات التي تم استخدامها في العملية التعليمية خلال العقد الأخير من القرن العشرين وأوائل القرن الحادي والعشرين"(12).

كما " يطلق على الشبكة الدولية (الإنترنت) الطريق الرقمي أو شبكة المعلومات الرقمية أو طريق البيانات السريع أو فائقة السرعة. هذا بالإضافة إلى ظهور تعبيرات جديدة مثل: شبكة المعلومات الدولية. وهي ليست شبكة واحدة قائمة بذاتها، وإنما هي شبكة من الشبكات التي تتبادل المعلومات والأفكار والآراء والبيانات والحقائق فيما بينها دون قيد أو شرط أو رقيب للأفراد في أي عمر أو عقيدة أو لون أو أية دولة في العالم"(13).

وهنا مكمن الخطر في تسرب المعلومات وتعرضها للسرقة، حيث إن الأمر أصبح مفتوح الأبواب، لا توجد ضوابط لمتى تفتح ومتى تغلق هذه الأبواب، إلا بوجود شركات متخصصة في الأمن المعلوماتي، يجب الاتفاق معها وفق شروط

دقيقة ومفصلة. فبالاتفاق مع هذه الشركات سوف نحقق أمرين، الأول: المحافظة على معلوماتنا من الضياع والسرقة، والأمر الآخر هو: الحصول على معلومة صحية وموثقة من مصادرها الأصلية محفوظة الملكية؛ فـ "لم يعد هدف التربية المعاصرة تحصيل المعلومات فقط، حيث لم يعد تحصيل المعلومات هدفا في حد ذاته، بل الأهم من تحصيلها القدرة على الوصول على مصادرها الأصلية وتوظيفها لحل المشكلات. ولم يعد وظيفة التعليم مقصورة على تلبية الاحتياجات الاجتماعية والمطالب الفردية، بل تجاوزتها إلى إكساب الإنسان القدرة على تحقيق ذاته وأن يحيا حياة أكثر ثراء في الفكر والمعرفة"[14].

الأمن المعلوماتي: لعل البعض يرى بأنه لا توجد اعتبارات قانونية "لأن المحاكم لم تفصل حتى الآن في كثير من القرارات القضائية عما هو قانوني على الإنترنت"[15].

إن وضع أي تشريع قانون لاستخدام الإنترنت لا يقتصر على الأمن المعلوماتي والحقوق الفكرية وحقوق المؤلف والحقوق المجاورة، فهذه جزئيات في التشريع وإن كانت مهمة جدا؛ إلا أن هناك مخالفات جسيمة تمس الأخلاقيات الأدبية غير العلمية، وهناك خروقات لاتفاقيات تسيء للمجتمعات والدول.

وأما فيما يتعلق بالمعلوماتية فـ "إذا كان لدينا شك إذا كنا نحتاج لإذن لاستعمال شيء على الأنترنيت، نحصل على الإذن. وإذا كان لدينا إحساس أننا على أرض غير قانونية، نستشير محام، ومع أن الاستشارات القانونية مكلفة؛ فإن تكاليف الأعمال القانونية ستفيدنا بكل تأكيد"[16].

يضرب لنا أحد الباحثين مثالا فيما يخص (مواد حق النشر) حيث يقول "الخاصية الفكرية والمحتمل أن نقوم بها هي مواد حق النشر. فإذا جعلنا مستندات

متاحة لمستعملي الأنترنيت، نحتاج لحق نشر المستندات التي نرغب في التحكم فيها. والحصول على حق النشر متاح. نسلم نسختين من المستندات لمكتب حق النشر في الولايات المتحدة (us) في خلال ثلاثة أشهر من النشر الأولى، ونعرض معلومات حق النشر بوضوح في المستند... وحقوق النشر فعليا أو أوتوماتيكية؛ فمجرد أن نضع مستند فهو ملكنا (إلا إذا وافقنا مع بعض آخر مع مثلا موظف). وتسجيل مستتدنا مع مكتب حقوق النشر يساعد في إثبات أننا أصحابه. ويجب التأكيد من تسجيل مستنداتنا قبل جعلها متاحة للآخرين على الأنترنيت حتى لا يسجلوه قبلنا. وتظل حقوق النشر ذات قوة لمدة خمسين عاما بعد موت المؤلف (أو إذا كان مشاركا مع مؤلف آخر، أي بعد وفات آخر مؤلف هي لهذا المستتد) والشركات تظل حقوق النشر لفترة مئة عام بعد عمل المستند، أو بعد 75 عاما بعد نشره، أيهما أقصر"[17].

ومن أخلاقيات نقل المعلومات من الأنترنت "لا يمكننا قطع وتجميع أجزاء من عمل شخص آخر وتغيير بعض الكلمات هنا وهناك. وهذا الانتهاك يسمى (fairuse)، والي يمكن عمله، هو استعمال أفكار أحد الأشخاص، وإذا وضعنا هذه الأفكار بكلماتنا نحن، لا يمكن لأحد أن يشكو أنه صاحبها. ويمكننا أن نختار لتضمين بعض المراجع للمستند الآخر في بيان المؤلف"[18]، السرقات العلمية عرفت قديما – لاسيما – عند الشعراء، وهناك مؤلفات كبيرة وكثيرة تخصصت بالسرقات الأدبية والشعرية، لسنا في مجال ذكرها، فمن الممكن حتى من قراءة الكتب الورقية تتم السرقة، وهناك كثير من الجوائز الأدبية سحبت أو حجبت عندما اكتشفت لجنة التحكيم سرقة المعلومات فيها، وكذلك بالنسبة للأفكار تعد أيضا سرقة، ولكن من الذي يضبط السرقات الفكرية إذا تشبث كل طرف بأحقيته

بالفكرة؟ كما أن هناك صيغا متفق عليها وكلمات الكل يستخدمها فهي ليست ملكا لأحد حتى يدعي من يدعي بأنها ملك له أو هو من استعملها؛ فلا يمكن أن استخدم عبارة "واضحة وضوح الشمس في رابعة النهار" ثم يأتي من يأتي ليدعي أنها عبارته أو هو أول من استخدمها، ولعل كثير من الناس يذهب بأن صدر البيت الذي استخدمه الحجاج بن يوسف الثقفي وهو (أنا ابن جلا وطلاع الثنايا) هو للحجاج، ولا يعلم بأن قائله شاعر جاهلي قديم.

الآن وقد بينا ما لدينا من معلومات خاصة في علم المكتبات (كتب مؤلفة رسائل وبحوث، دوريات وحوليات، مراجع ومصادر)، وأوضحنا شيئا من أخلاقيات نقل المعلومات، ثم بعد ذلك طالبنا باعتبارات قانونية (تشريع) للقرصنة الإلكترونية، جاء دور كيف نحافظ – نحن المعنيين في علم المكتبات – على هذه المعلومات في ظل مقولة "كل شيء على الأنترنيت يبدو حرا، وكل شخص يمكنه الوصول لأي شيء"[19].

في خبر نشرته الصحف حول شراء شركة (مايكروسفت) لشركة أمن المعلومات الإسرائيلية (أدالوم) مفاده أن الشركة "توفر تكنولوجيا أمن معلومات المستخدمين على الخادمات البعيدة. وتستطيع تأمين المعلومات المخزنة على الإنترنيت لشركات "سيزنورسي" و"مايكروسوفت" و"غوغل" وحمايتها من الهجمات الرقمية. وأبرمت عملاقة التكنولوجيا الأميركية عدة صفقات استحواذ في إسرائيل في الفترة الأخيرة. منها شراء شركة البرمجيات الأمنية (أوراتو) في صفقة أفادت تقارير بأن قيمتها 200 مليون دولار. واشترت أيضا شركة تحليل النصوص (إكويفيو) وتكنولوجيا شركة (إن – تريج) للتعلم الرقمي".

ما يعني أننا بحاجة إلى إنشاء شركات خاصة لأمن المعلومات وفق ضوابط ومعايير دولية ورؤية عربية إسلامية مشتركة ورؤية وطنية خاصة وهذا – لاشك – بأنه سوف يفتح الباب على مصراعيه للمستثمرين كما أنه سوف يفتح الباب لمقررات جديدة تدرس في الجامعات والمعاهد، وبالتالي سوف يوفر فرص عمل وبذلك نكون قد عملنا تحت مظلة قانونية آمنة، والحماية هذه كما يراها بعض الباحثين "عبارة عن برنامج تطبيق والذي يوضع على حاسب آلي بين شبكتنا المحلية والأنترنيت، ويجب أن تمر كل رسائل الأنترنيت عبر الحماية"[20].

وقد دعت الحاجة أيضا لإنشاء شركات أمن معلوماتي "لأن الخوف من تجسس المشتركين في انترنت، ومن التخريب، وسرقة الهوية الذاتية، والاعتمادات المالية وفقدان سرية المراسلات واحتمال نفوذ الآخرين إلى السرية والخاصة، وكل ذلك أفضى إلى الحذر من الاقتراب من الخدمات المباشرة التجارية، ولبعض هذه المخاوف أساس، إلا أن بعضها الآخر اختفى تماما، فقد تعاونت المؤسسات البرمجية الكبرى بهدف وضع بروتكولات أمنيـــة بمستويات مختلفة، لتحقيق أهداف متعددة للأمن الخاص في المؤسســـات، وهكذا أمكن تفادي مثل هذا النفوذ عن طريق إنشاء نظام حاجز حماية (FIRWALL) تمرّ عبره الملفات والمعطيات ذهابا وإيابا" [21].

ملحق

– **أخلاقيات الإعلام:** " أحد برامج اليونسكو، من مهامه المتعددة " تحديد القضايا الرئيسية ذات الصلة بإنتاج المعلومات والوصول إليها ونشرها وحمايتها واستخدامها في بيئة إلكترونية .. عقد أول مؤتمر حول أخلاقيات الإعلام في شهر مارس / آذار 1997، بموناكو. ومن المواضيع التي تناولها المؤتمر الوصول إلى المعلومات في إطار أخلاقي.. وحماية المعلومات والوثائق الرقمية"[22].

– **ذاكرة العالم:** "ذاكرة العالم – أحد برامج اليونسكو" يتمثل الهدف الأول في حماية تراثنا الوثائقي ذي الدلالة العالمية وتشجيع حماية تراثنا الوثائقي 1ي الدلالة الوطنية والإقليمية وذلك بأنسب الوسائل"[23].

– **مكتبة المتوسط الافتراضية:** "مكتبة المتوسط الافتراضية" تهدف أساسا إلى جمع التراث الوثائقي للبحر المتوسط على شبكة الإنترنيت سواء تم إنتاجه داخل المنطقة أو خراجها"[24].

– **شبكة اليونسكو للمكتبات المشاركة:** "شبكة اليونسكو للمكتبات المشاركة (UNAL)**:** أحد برامج اليونسكو، لدعم التعاون من أجل التفاهم الدولي – في تشجيع المكتبات العامة على القيام بأنشطة ذات صلة بمهمة اليونسكو .."[25].

– **تعلم بدون حدود:** "تعلم بدون حدود: أحد برامج اليونسكو: تهدف إلى دعم نظم التعليم المتنوعة والمفتوحة في اتجاه التعلم مدى الحياة مؤكدة على المساهمة المحتملة لتكنولوجيا المعلومات والاتصال الجديدة في خلق بيئات تعلم ملائمة وذات معنى حيث توفر تكنولوجيا المعلومات والاتصال فرصا لمزيد من المرونة"[26].

– **مراكز المجتمع الريفية ذات الأهداف المتعددة للاتصال عن بعد في إفريقيا:** "مراكز المجتمع الريفية ذات الأهداف المتعددة للاتصال عن بعد في إفريقيا. أحد

برامج اليونسكو، يمكن النظر إلى مثل هذا المركز على أنه مكتبة المستقبل للمجموعة تدعم هدف الوصول الكوني لمجتمع المعلومات الناشئ"[27].

الخاتمة: من الغريب العجيب أن نرى مكتبة تابعة لمعهد دولي تابع لمنظمة عربية منبثقة عن جامعة الدول العربية، مازالت تعمل بالطرق التقليدية؛ فلو كانت مكتبة عامة أو حكومية أو مدرسية أو خاصة للمسنا لها العذر في قلة الإمكانات المادية أو قلة الخبرة، وندرة الكوادر المتخصصة، أما أن تكون مكتبة تابعة لمعهد دولي تابعة لمنظمة عربية تضم في عضويتها اثنتين وعشرين دولة عربية، لها ميزانية خاصة ولها حصص كبيرة من الدول، ومازالت في المرحلة الأولى في التوجيه نحو العمل المكتبي الإلكتروني – حقيقة – لا أجد عذرا أو مبررا لذلك! ولكن الأمل موجود ونظرة التفاؤل ثرة دائما وأبدا والتوسم خيرا بمن يتبؤ كرسي إدارة المعهد.

لعلي لا أبالغ إذا قلت إن مكتبة معهد الخرطوم الدولي للغة العربية تفوق في قيمتها المعرفية مكتبات عربية مرموقة، وقد تزاحم المكتبات الدولية في مدى الحاجة إليها. ولا يقلل من قيمتها مبناها المهترئ، ولا يغض من مكانتها المعرفية طريقتها التقليدية في حفظ الكتب وتصنيفها، ولكن نحن دائما وأبدا نطمح بالكثير لم لا؟! لطالما لدينا هذا الكنز من الكتب والمجلات والدوريات والحوليات والمراجع والمصادر؛ لم لا نفتح المجال على مصراعيه للاستفادة منها للقاصي والداني؟ لماذا لا نبحر بهذا الكنز إلى أصقاع الأرض ليطلع عليه ويتمتع به من أراد له ذلك؟ لم لا نتجول به في الفضاء الطلق لنشره على الملأ؟ لماذا هذا الكنز حبيس الأرفف

الحديدية القديمة؟! ولطالما دولة المقر جمهورية السودان – مشكورة – لم تدخر أي جهد إلا وبذلته في سبيل رقي هذا المعهد والمحافظة على نهجه وكنزه.

آن الأوان أن نجعل من مكتبة معهد الخرطوم الدولي للغة العربية مكتبة رقمية وافتراضية وإلكترونية، آن الأوان أن ننهض بها إلكترونيا، آن الأوان أن نتجه بها نحو التطوير ونحو العالمية.

الطريق نحو عالم المكتبات الرقمية: لمسنا ونحن في السودان أن هناك طاقة بشرية عاملة وعالمة، تتمتع بمستوى مهني وتقني، ولعل حب السودانيين للعلم والمعرفة – ولاسيما – شغفهم النادر بتعلم اللغات جعل منهم عملة علمية نادرة تتهافت عليها الدول – وعلى وجه الخصوص دول الخليج العربية – فلا يختلف اثنان على أن السوداني جاد في عمله، متقن لتخصصه، متحصن بثقافة عالية.

إن العمل على جعل مكتبة معهد الخرطوم الدولي للغة العربية مكتبة رقمية ينطلق من ثلاث سياقات مهنية:

1- أمين مكتبة متخصص في علم المكتبات (دراسة أكاديمية).

2- دكتور متخصص في علوم اللغة العربية والتربية.

3- معلوماتي إلكتروني في تصنيف علم المكتبات الإلكترونية.

"فالمكتبات اليوم هي بوابات لجادة المعلومات. فهي لا تشتغل كهيئات منفصلة ولكن كأجزاء من شبكات محلية وكونية ذلك أن الرقمية وربط الشبكات يجعلان من المكتبات الوطنية مثلا وللمرة الأولى بحق تتصل بكافة الناس والجهات في القطر"[28].

ولعل خير ما نختتم به هذه المداخلة توصية لأحد الباحثين حيث يوصي "الكليات والأقسام التي تدرس علم المكتبات والمعلومات بإعطاء موضوع البحث في قواعد

البيانات أهمية خاصة نظريا وعمليا وأن تعمل على تحمل مسؤوليتها في تطوير الملاكات الوظيفية التي لم تسنح لها الفرصة بالتعرف على هذا النوع من الخدمات وذلك بالحصول على دورات تدريبية وبشكل مستمر لزيادة مهاراتها وتطوير إمكاناتها، ليصبح المكتبي مؤهلا تأهيلا علميا وعمليا لإجراء هذا النوع من الخدمات التي لا تخلو منها المكتبات الحديثة"[29] .

الهوامش:

---

1 – انظر: جهود معهد الخرطوم الدولي للغة العربية في كتابة لغات الشعوب الإسلامية بالحرف العربي: أ.د. علي عبدالله النعيم، مدير معهد الخرطوم الدولي للغة العربية، المجلة العربية للدراسات اللغوية، مجلة علمية محكمة نصف سنوية يصدرها معهد الخرطوم الدولي للغة العربية العدد: 35 صفر 1436 هـ – ديسمبر 2014 م، ص 143 .

2 – انظر: المكتبة الجامعية وتحديات مجتمع المعلومات، السعيد مبروك إبراهيم، دار الوفاء لدنيا الطباعة والنشر والتوزيع، الطبعة الأولى 2009 م، ص 3 .

3– انظر: خليفة الوقيان...

4 – انظر: إدارة المعرفة ودورها في إرساء أسس مجتمع المعلومات العربي، د. عماد عبدالوهاب الصباغ، المجلة العربية للمعلومات، عدد 2، تونس 2002، المنظمة العربية، ص 37.

5 – انظر: المرجع السابق ص 40 .

6– انظر: دليل معهد الخرطوم الدولي للغة العربية – السودان الخرطوم يوليو 2014 م.

7 – انظر: تجربة معهد الخرطوم الدولي للغة العربية 29 عاما من العطاء، إعداد: أ.د. عبد الهادي تميم، الخبير الأول بالمعهد. وثائق اجتماع مديري معاهد تعليم وإعداد معلمي اللغة العربية للناطقين بلغات أخرى، المنعقد في الخرطوم – السودان في الفترة من 21 – 23 شوال 1424 هـ – 15 – 17 ديسمبر 2005 م. ص 365 .

8 – انظر: جهود معهد الخرطوم الدولي للغة العربية في كتابة لغات الشعوب الإسلامية بالحرف العربي: أ.د. علي عبدالله النعيم، مدير معهد الخرطوم الدولي للغة العربية، المجلة العربية للدراسات اللغوية، مجلة علمية محكمة نصف سنوية يصدرها معهد الخرطوم الدولي للغة العربية العدد: 35 صفر 1436 هـ – ديسمبر 2014 م، ص 143 .

9 – انظر: المكتبة الجامعية وتحديات مجتمع المعلومات، السعيد مبروك إبراهيم، ص 11 .

10- انظر: إدارة المعلومات في بيئة الرقمية، - المعارف والكفاءات والجودة، تونس 2003 المنظمة العربية للتربية والثقافة والعلوم، الاتحاد العربي للمكتبات والمعلومات، ص 36 .

11 - انظر: تقييم لمواقع المكتبات على شبكة الإنترنت: المعايير العددية والنوعية، المكتبة الرقميـــة الدوليـــة للأطفـــال وبحـــوث أخـــرى، د. سهيـــر أحمـــد محفـــوظ، درا الثقافة العلمية، 2009، ص 19 .

12- انظر: المكتبة المدرسية والوسائط الإلكترونية، ص 69 .

13- انظر: المرجع نفسه، ص 69 .

14- انظر: المكتبة المدرسية والوسائط الإلكترونية قضايا ومشكلات تربوية وتكنولوجية، فهيم مصطفى، سلسلة دراسات في علوم المكتبات والمعلومات، 2006، دار الفكر العربي، ص 30 .

15- انظر: الأنترنيت: الشبكة الدولية للمعلومات، م. فاروق سيد حسين، دار الراتب الجامعية بيروت، 1997 م، ص 144 .

16- انظر: الأنترنيت ص 144 .

17- انظر: فاروق سيد حسين، ص 148 .

18- انظر: فاروق سيد حسن، ص 149، ا.

19- انظر: فاروق سيد حسين، ص 148 .

20- انظر: فاروق سيد حسين، ص 152 .

21 - انظر: الانترنيت، إمكاناتها، أدواتها وجدواها في المكتبات العامة، أ.د. عبداللطيف صوفي المجلة العربية للمعلومات، المجلد التاسع عشر، العدد الثاني، تونس 1998، المنظمة العربية للتربية والثقافة والعلوم، ص 29 .

22 - انظر: أ. عبدالعزيز عبيد، ص 92 .

23- انظر: أ. عبدالعزيز عبيد، ص 92 .

24- انظر: أ. عبدالعزيز عبيد، ص 94 .

25- انظر: أ. عبدالعزيز عبيد، ص 95 .

26- انظر: أ. عبد العزيز عبيد ص 96 .

27- انظر: أ. عبدالعزيز عبيد، ص 97 .

28- انظر: اليونسكو، المكتبات العمومية ومجتمع المعلومات، أ. عبدالعزيز عبيد، المجلة العربية للمعلومات، 19 - 2 - تونس 1998، ص 87 .

29- انظر: استراتيجيات البحث وتطبيقاتها في قواعد البيانات على الأقراص المكنزة: دراسة تجريبية على قاعدة بيانات مركز مصادر المعلومات التربوية (ERIC)، أ. طلال ناظم الزهيري ص 101 . مجلة المعلومات، المنظمة العربية ص 121.

مهددات الهوية الجزائرية والجرائم الالكترونية بين التشريع والتطبيق

أ.بوخاري مليكة

المدرسة الوطنية العليا لعلوم الإعلام والصحافة (الجزائر العاصمة)

مفردات البحث: استهداف الإسلام، مقومات الهوية الجزائرية، صورة الفتاة الجزائرية، الثقافة الجزائرية، اللغة، الحرية الفردية، الحق في الصورة، الحرية الفردية.

مقدمة: يعد الحاسوب مسرح الجريمة وكذا مسرح لاكتشاف من وراء الجريمة أيضا من خلال مختلف الأساليب التي تتبع من طرف المصالح الموكل لها التحقيق والتقصي في مثل هذه الأنواع من الجرائم التي تعد اليوم من الجرائم المنظمة والعابرة للقارات كما تستخدم الجريمة الالكترونية أيضا في الحرب الدعائية الالكترونية بين الدول وقد تلجأ بعض الدول إلى مس مقومات دول أخرى لأهداف سياسية واقتصادية كما أن الأفراد فيما بينهم يستغلونها لأغراض مختلفة.

رغم أن الضرر المادي لمثل هذه الجرائم كبير إلا أن الضرر الذي يمس بالهوية للبلدان أو للمقومات يعد أكبر وأعظم من خلال التشويه الذي يطال مجتمع ما من خلال ما يبث عبر الانترنت باعتباره مخزن للمعلومات أو حتى تمرير إشاعات حول مجتمع ما وسنحاول أن نتعرض لمختلف ما يهدد مقومات هوية دولة ما على غرار **الإسلام** مثلا كما نتطرق للمعلومات التي تعرض حول الفتاة

الجزائرية **والحجاب** وغيرها من مقومات المجتمع الجزائري من تهديد وتشويه من جهة كما سنتطرق لحق الفرد في الحفاظ على حريته الفردية في مجتمع عالمي افتراضي وكذا الحق في الصورة وهو حق مضمون لكل إنسان.

1- سلطة الانترنت في المجتمعات ما بعد الحداثة: إذا كان التطور التكنولوجي هو مجرد حصيلة للمعرفة الإنسانية فإن سمته في عصرنا الحالي هي التواصل الكبير والذي يقوم على أساس التقنيات المتطورة جدا في حقل الإعلام والاتصال خاصة، وهو ما بشر به **مارشال ماكلوهان** في الستينات من القرن الماضي عن ما يعرف "**بالقرية الكونية**" وهو في الواقع ما نعيشه اليوم بفضل الانترنت وما توفره من خدمات متعددة ومواقع رائدة تأتي في مقدمتها المواقع الاجتماعية التواصلية **كفايس بوك** والذي يأتي في مقدمة المواقع الأكثر استعمالا ثم موقع "**ماي سبايس**" و"**التويتر**" والتي تتيح اليوم للإنسان المسلم التواصل مع مختلف الجنسيات والديانات وهو مكسب يجدر بنا الاستفادة منه "فبظهور الانترنت زادت فرص الحوار والتواصل الإنساني بين البشر جميعا على وجه الأرض عبر الفضاء الافتراضي الالكتروني أو فضاء المعلومات وهو بيئة متعددة الجوانب، معقدة بقوة، نشأت من أشكال لا يمكن تخيلها من الحياة الرقمية، وظهرت كيانات اجتماعية مفترضة لم تكن موجودة في السنين القليلة الماضية."[1]، والكل يتفق على أن ميزة المجتمعات ما بعد الحداثة هي التكنولوجيا وسلطة المعرفة فتغيرت مفاهيم القوة والسيطرة باعتراف زعماء الدول أنفسهم وننقل شهادة للرئيس الأمريكي السابق **بال كلينتون** والذي قال "في عدد مارس – أبريل لسنة 1996 لمجلة **فرين أفيرز:** المعرفة هي أكثر من أي وقت مضى سلطة، فالدولة التي ستتزعم ثورة الإعلام هي التي ستكون قوية بين الدول، على المدى المنظور هذه الدولة هي الولايات

المتحدة، هذه السلطة اللامادية ستمكننا من التحكم في العلاقات الدولية بالجذب لا بالقوة، بالتالي فلا مجال لتحمل تكاليف عسكرية جديدة."[2] هو اعتراف يوضح لنا نحن كعرب ومسلمون فرص نجاحنا الضئيلة خاصة وان نسبة الأمية المتزايدة في المجتمعات العربية يجعل المعرفة بالمفهوم الحداثي بعيدة عنا **والعراق** نموذج حي في حين الأمم المتقدمة تتقن لغة الانترنت اليوم أي أننا لابد أولا من إتقان اللغة التي يتحدثها ويتواصل بها العالم حتى نستطيع أن ندافع عن معتقداتنا وتفكيرنا وحضارتنا العربية الإسلامية الأصيلة وبصورة ملحة الدفاع عن الرسول صلى الله عليه وسلم لاسيما مع تنامي الكره الذي يكنه الغرب للمسلمين وللرسول وإلصاق الصورة النمطية بنا كمسلمين مع كل السلبيات التي تساهم في تكريس التصور القائم حولنا بمختلف الوسائل الحديثة خاصة ما تعلق بوسائل الإعلام والاتصال، في ظل معطيات لا تخدم تصورنا الروحي المعنوي فالجانب المادي والغرائزي بات المسيطر على كل مناحي المجتمعات الالكترونية والتي تحدث عنها الباحث الأمريكي **بريجنسكي** "ففي مشروع هذا الاستراتيجي الأمريكي تنتفي القوة الأمريكية بمعناها القديم لتستحضر الطاقات الحربية الجديدة في المجتمع النكتروني كما يسميه المجتمع الذي تتشكل ثقافيا ونفسيا واقتصاديا بتأثير التكنولوجيا والالكترونيات ويكون في إمكانه ليس سيادة النمط الأمريكي وشيوعه الذي يلح عليه **كرافت،** فذلك مجرد انطباع خارجي كما يراه بريجنسكي وإنما انجاز الثورة الثالثة حيث تتمكن أمريكا في مجتمع **نكتروني** عالي التطور على مد نفوذها غير المرئي إلى كل المجتمعات بهدف إخضاعها كلية."[3] ولعل احتكار التكنولوجيا من طرف شركات عالمية هو دليل على تبعية باقي الدول لهذه الإمبراطوريات وعن سياق وسائط الإعلام الحديثة يقول الخبير في العلاقات الدولية **محمود الفطفاطة**

"ابرز صور **اللاديمقراطية الالكترونية** في العالم والتي تجسدها الولايات المتحدة الأمريكية فأمريكا تحتكر تكنولوجيا الحاسوب والانترنت بصفة خاصة مثل ما يحدث بين الشركات الأمريكية العملاقة مايكرسوفت غوغل نيتسكيب صن سيستمز(...) وتدير من خلالها توجهاتها المعلوماتية على صناعة تكنولوجيا المعلومات وعالم الانترنت"[4]. وأكثر من هذا في حولت الانترنت إلى وسيلة دعائية ومن بين اخطر وسائل الحرب السلمية أو ما يعرف بالقوى الناعمة التي لا تسيل دماء واقعية وإنما تحول أجيالا كاملة إلى تماثيل تتلقى معاني الحضارة والهوية والانتماء عبر شبكة الانترنت العالمية.

2- الجريمة الالكترونية وأنواع المجرمين على شبكة الانترنت: لنتمكن من تفكيك العلاقة الموجودة بين الهوية الوطنية والجريمة الالكترونية لا بد أولا من تحديد وتعريف الجريمة الالكترونية من الناحية القانونية وأيضا من الناحية القيمية لنربط هذا النوع من الجرائم الذي يرتكب افتراضيا غير أن تأثيراته تكون على المجتمع الفعلي وخيمة أيضا والملاحظ أن الأساس الذي يعتمده الخبراء هو الأثر المالي لهذه الجريمة والتي تعتبر في المقام الأول أساسها الربح المالي سواء بالنصب والاحتيال أو بسرقة أموال من البنوك والمؤسسات أو المساومات المالية على المعلومات الشخصية بنشر الصور الخاصة بالأفراد أو التهديد بفض المعلومات الشخصية، "فتعرف جرائم الانترنت أنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة في الكمبيوتر والانترنت في أعمال وأنشطة إجرامية بعد فان تحقق عوائد مالية ضخمة يعاد ضخها في الاقتصاد الدولي عبر شبكة الانترنت باستخدام النقود الالكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الانترنت أو التداول الأسهم وممارسة الأنشطة

التجارية عبر هذه الشبكة وقد عبر خبراء المنظمة الأوربية للتعاون الاقتصادي عن جريمة الانترنت بأنها كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها."[5].

وفي تعريف أكثر دقة يقترب من النقاط التي نتناولها في المداخلة فيمكن أن نعرف الجريمة الالكترونية بأنها "**تعني جرائم الشبكة العالمية التي تستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب.**"[6]

ويلخصها المنسق الفني **ياحي احمد** لمجلة الشرطة الجزائرية "هي أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها سواءً كان ذلك بطريقة مباشرة أو غير مباشرة وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الانترنت غرف الدردشة أو البريد الالكتروني أو المجموعات"[7]، ويضيف عن أنواع الجريمة الالكترونية فيمكن أن نصنفها كما يلي:

"القرصنة والاختراقات الالكترونية، السب والتشهير عبر الانترنت، صناعة ونشر الفيروسات وهي أكثر الجرائم انتشارا وشيوعا على الانترنت، انتحال الشخصية، تشويه السمعة وذلك بنشر معلومات حصل عليها المجرم بطريقة غير قانونية وتكون هذه الأعمال لأهداف مادية أو سياسية أو اجتماعية، النصب والاحتيال كبيع السلع أو الخدمات الوهمية."[8]

ويمكن أن نقسم ونصنف من يقومون بالجرائم الالكترونية إلى أصناف متعددة من **هاكرز** أي قرصان وأيضا ما يعرف **بالكريكرز** ويمكن تصنيف القراصنة إلى ثلاث أنواع نظرا لكونهم الأكثر تمكننا في المجال التكنولوجي وفي مجال قرصنة المعلومات وتحويلها ونقصد بالمعلومات كل ما هو غير قابل للنشر كالصور

والمحادثات وكذا الفيديوهات أو حتى المواقع الهامة للمؤسسات أو البنوك أو حتى مواقع الوزارات أي كل معلومة يمكن أن تحول إلى مصدر مساومة أو ابتزاز على حسب نوع القرصان[9] :

أ – **القراصنة أصحاب القبعات السوداء:** يمكن أن نصنف هذا النوع من القراصنة **بالكريكرز** وهم أشخاص متمكنين من الحاسوب وأنظمته بشكل كبير ويقومون بقرصنة المواقع الالكترونية وأيضا بتعطيل البرامج التي يحاولون وهم لا يحترمون القوانين وعادة تكون هذه الفئة هدفها مادي ويقتربون من الكريكرز الذين يصنعون الفيروسات وينشرونها في الانترنت لتدمر المعلومات ويطلق الأخصائيين على هذا النوع من المجرمين الارهابين أو الجريمة الإرهابية عبر الانترنت. ويمكن أن ندرج هذا النوع من القراصنة فيما يعرف بحرب المعلومات التي تشن اليوم بين الدول من خلال التحكم في نشر المعلومات والتسويق لأخرى وكذا اختراق خصوصيات الدول على كل المستويات.

ب– **القراصنة أصحاب القبعات البيضاء:** هذا النوع يقترب من النوع الأول غير أن الاختلاف يكمن في الأهداف التي يتبناها قراصنة القبعات البيضاء حيث يقوم هذا النوع من القراصنة باختبار الأنظمة والبرمجيات ومحاولة اكتشاف الأخطاء الموجودة فيها ونشرها حتى تتمكن المؤسسات من إدراكها للفجوات التي يمكن أن يتسلل منها القرصان الأسود غير أن هذا الأخير وحين يكتشف الفجوة لا ينشرها أبدا بل يقوم بمحاولة استغلال أي نقطة ممكنة بغرض الربح المادي أو بيع المعلومات لجهات أخرى منافسة مثلا.

ج– **القراصنة أصحاب القبعات الرمادية:** يتقاطع هذا النوع مع النوعين الأولين حيث يقوم هذا القرصان الهجين بأعمال مثل قراصنة القبعات البيضاء لكنه في

بعض الأحيان يتحول لقرصان أسود لما يحتكر بعض المعلومات حول البرمجيات لأغراض شخصية عادة.

3 – تهديد ثوابت الهوية الوطنية من خلال الجرائم الالكترونية: إن مسالة الهوية في العالم تطرح نفسها كمشكلة أساسية في بناء الأمم من حيث الترابطات الكبيرة المتعلقة بمسالة الهوية فهناك من يرى أنها مجرد تصور فكري يتغير بتغير الزمن غير أن هذا الطرح والذي يتبناه المفكر الهندي **مدان صاروب** الذي يطرح إشكالية الهوية الكاملة والتامة والتي تبني حسب من خلال القصص المتوارثة عن أنفسنا وهو طرح يستند إلى أسس عقلية منطقية غير أن السياق الذي يتناول فيه الباحث حديثه عن الهوية هو بالفعل النسق الهندي أين يتداخل الروحاني مع المادي مع الأسطوري غير أن المجتمعات الإسلامية هي غير ذلك نظرا لنظرتنا نحو الدين مثلا وقداسة قيمه، وموضوع الهوية لطالما كان موضوع سجال بين الهوية القومية وهويات الأقلية غير أن الموضوع الذي نتطرق إليه هو موضوع ثوابت الهوية الأساسية كالدين الإسلامي مثلا، والذي يتعرض إلى حرب ضروس تشوهه ومن خلال ذلك تشوه صورة المسلم والقيم التي يتبناها تصبح تحصيل حاصل لكل قيم الدين ومقومات أمة بكاملها، وما يتوجب علينا أساسا هو الحفاظ عن هذه القيم التي تعد من ثوابت الأمة الجزائرية .

أ– الهوية الوطنية والانترنت: إن تطور المجتمعات العالمية وعلى الأقل الصناعية وما يعرف بالمجتمعات ما بعد الحداثة تدفعنا إلى محاولة معرفة نصيب الدول العربية النامية من المثاقفة وما هي تداعياتها على الهوية في عالم اليوم الذي لا يعترف بالقيم والروحانيات لأنه في الأساس عالم مبني على أسس نيوليبرالية مبادئها معروفة بماديتها، ودول المغرب العربي من الدول النامية والتي تسعى إلى

الاتحاد ولو بشكل نظري وهو في الحقيقة ما تفرضه الظروف العالمية القائمة اليوم حسب المختصين يؤكدون أن " الدراسات المستقبلية التي عالجت النظام العالمي عن البدائل المطروحة ضمن مشاهد مستقبلية وعن أنماط للتفاعلات تحدد شكل العلاقات الدولية مستقبلا وهي نظام التعاون والتنافس ونظام التوتر والردع ونظام العنف والحرب."[10]، لهذا أصبح لزاما على بلدان المنطقة التعاون وخاصة في مجال حماية القيم، من تعاون تسمح به التقنيات الحديثة على غرار الانترنت غير انه من الضروري أن تحافظ على خصوصيتها الإقليمية وهو ما جاء به **رجب بو دبوس** في كتاب **محاكمة العولمة** حيث يرى "إن توطين التعليم هو تحرير التعليم من دكتاتورية السوق التي تجعل منه تجهيلا إجباريا (...) هذا بالطبع لا يعني قطيعة مع بقية العالم، الاتصال يجب أن يستمر بفضل تبادل ثقافي وتبادل خبرات والذي يمثل جزءا مهما في عملية التعليم."[11].

أما فيما يخص المثاقفة الغربية فيجب أولا أن نحدد مفهوم المثاقفة الذي يحدده **فيصل دراج** فيقول "تتعين المثاقفة نظريا بحوار ثقافة محددة مع ثقافات مغايرة لها بحثا عن عقل ثقافي جماعي، يرى في المشاركة العادلة مبدأ، ويرى إلى خير إنساني مشترك. لكن ما يبدو واضحا وبسيطا قوامه ثقافات مستقلة تحاور بعضها يتكشف أكثر صعوبة مما يبدو بسبب شروط الحوار الثقافي، بلغة معينة أو المثاقفة بلغة أخرى أكثر دقة."[12] غير أن المثاقفة اليوم تعني فرض الثقافة بما فيها التربية من الشمال على الجنوب وهناك استبداد وهيمنتها أو محاولتها القضاء على باقي الثقافات الوطنية لهذا تصبح اليوم التربية من محركات الحفاظ على الدولة أو الأمة واليوم لا تعيش الإنسانية المثاقفة بمعناه الايجابي الذي يتضمن التبادل والعدل والمساواة بين منظومتين هما المنظومة المعرفية المبنية على الخطأ والصحيح

والمنظومة الأخلاقية التي تحيل إلى "الشر أو الخير وهذه الأخيرة تختلف لأن المعتقدات متغايرة تماما وإذا كانت الدول تهدف حقا للمثاقفة فلابد من تحترم جملة المعتقدات التي لا تتوافق معها لا أن تحاول القضاء عليها كما هو الحال اليوم من محاولة إلى قولبة كل العالم في نموذج أحادي منط" لا يقوم الإشكال في المنظومتين السابقتين المختلفتين بل في تأويل نتائجهما الذي يستولد المثاقفة السوية أو يلغي شروطها فإذا كان الاعتراف المتبادل بين الهويات الثقافية المتغايرة شرط المثاقفة ومقدمة لها فإن انقلاب مقولتي الخير والشر إلى مقولتي الأقوى والأضعف يجتث المثاقفة ويفرض مرجعا ثقافيا وحيدا."[13] ولعل في الدول العربية هذا العنصر هو عنصر إنماء لا اختلاف نظرا للتقارب في المنظومات الثقافية والدينية والعقائدية إلى غيرها من مقومات تأسيس منهج قيمي يدافع عن هوايتها خاصة فيما يتعلق بالقيم الأساسية مثلا التربوي بعيدا عن الهيمنة، ما يحيلنا للحديث عن تحديات التربية في المغرب العربي وكيفية إرساء قيمه الحضارية، وفي وسط هذا النسق الذي نعيش فيه نلاحظ اليوم الكثير من التداخلات في هذا العالم الذي أصبح كالقرية الصغيرة وأصبحت هوية الأقليات في خطر من سلبيات العولمة التي تتحدى هذه الهويات الوطنية لصالح الأمركة " ففي زمن العولمة الذي اختزل كوكبنا إلى قرية صغيرة بالمفهوم الجغرافي المكاني لا الإنساني القيمي لم يعد يسمع إلا صوت القوي الذي يحاول غير أبه بشيء أن يجعل من وجوه الآخرين نسخا مكررة من وجهه وان يصبغ بفكره وفكر الآخرين ويفرض قيمه ونمط حياته على حوله وما حوله متخفيا خلفا أقنعة ظاهرها الديمقراطية والعدالة والمساواة والمصالحة وباطنها الاستبداد والظلم والتفرقة والإفساد"[14]، كما ان هذه العولمة مسؤولة بالدرجة الأولى عن كسر الحدود بين الأمم والأشخاص فالمجتمعات الالكترونية تنافس الصين مثلا

من التعداد البشري فعلى سبيل المثال مجتمع الفايس بوك وحسب الموقع الرسمي له فقد بلغ عدد المنظمين له أكثر من 1'32 مليار نسمة ما يعني أن قابلية التعرض للجريمة الالكترونية في مثل هذه المجتمعات وارد بدرجة أكبر خاصة حين نعرف أن مجتمع الفايس بوك مثلا هو مجتمع افتراضي نسبة كبيرة منه يضعون فيه معلومات شخصية تتعلق بالحرية الفردية على وجه الخصوص، كما ينم هذا المجتمع العالمي عن تداخل في معطيات المم من حيث الهوية ومظاهر التعبير عنها من خلال المدخلات التي نجدها على صفحات هذا المجتمع الافتراضي والذي يوصف بالمعقد لاسيما بالنظر للعدد الكبير للمشتركين فيه في حين ؟أن خصوصية كل مجتمع تختلف عن المجتمعات الأخرى فالهوية تعد بمثابة بطاقة تعريفية لكل مجتمع تميزه عن باقية الهويات العالمية فإذا كانت الهوية حسب الباحثة **سميرة علي جعفر** "إنها حقيقة الشخص التي تميزه وتتضمن ارتباط الفرد بماضيه وحاضره ومستقبله وإحساسه بالتفرد والاستقلالية ووعيه بذاته وبالآخرين وحاجته النفسية التي يتوقف عليها تماسكه الداخلي وأمر وجوده كما تتضمن نسق القيم الذي يوجه سلوكه على أساس من الالتزام و دور اجتماعي يقوم به الفرد أثناء تفاعله مع الآخرين"[15]، فإن كانت الهوية كل ما ذكر ما مقدار الجرائم التي من الممكن أن تمارس عليها من طرف الأشخاص أو التنظيمات وهل يمكن أن نتحدث عن نوع جديد من الجرائم المنظمة والتي تتجاوز حدود البلد لتصل إلى قيم المجتمعات الأخرى خاصة أن الجميع يتفق على أن الهوية تكون هوية فرد كما تكون هوية جماعة وهوية الفرد تكون بسيطة تلك هي الأقرب إلى الذهن والأكثر انتشارا كالصفات الفردية وهوية مركبة تلك التي تحدد اتجاهه مسار فكره عقيدته وانتماءه ومثل هذه الهوية هي التي تجمعه بغيره من الذين يشتركون معه في الاتجاه والفكر

والعقيدة والانتماءات وتميزه في الوقت نفسه بتلك الفروق أو التضاريس التي يشترك معه فيها"[16]، ومما سبق ذكره يمكن أن نستنتج أن لكل أمة هوية وطنية يجب أن تحافظ عليها لتضمن استمرارية التناقل بين الأجيال وحتى تكون هذه الأخيرة متشبعة من هويته الخالصة وليست منسلخة عن ماضيها الحضاري مهما كان بسيطا أو غير مهم بالنسبة لباقي الأمم والدين الإسلامي يشكل إحدى ركائز الهوية الجزائرية غير أنه في مفهومه المعنوي يتعرض أيضا لتشويه يمكن أن يتجاوز الجريمة الالكترونية بل قد يصل إلى حرب لتشويه الدين الإسلامي وهوية الجزائر أيضا من خلال الانترنت السلاح ذو حدين.

ب: الإسلام كركن أساسي للهوية، وتعرضه للجريمة الالكترونية: الإسلام دين الدولة الجزائرية وهو ما ينص عليه الدستور أيضا إن تشويه الدين الإسلامي والعداء له عبر الانترنت أو عبر مختلف وسائل الإعلام والاتصال هو واقع منذ عقود لعدة اعتبارات على غرار ما يعرف بصدام الحضارات ونهاية العالم المقدمة في أطروحة **فوكو ياما** القاضي بتفوق الرأسمالية كأرقى شكل تعرفه البشرية وكذا صامويل **هندغتون** بصراع الثقافة الغربية مع الإسلام والثقافة الكنفوشيسية باعتبارهما لا يندمجان مع الثقافة الغربية، وهي الأطروحات المتداولة في الغرب وما تمخض عنه الصراع والحوار الحضاري المبني في الأساس على مبدأ القوة والأكيد هو ليس في صالحنا كمسلمين أو حتى في صالح الإسلام وقضية الإساءة للإسلام أخذت منحى أخطر بعد تداعيات 11 سبتمبر 2001 في الولايات المتحدة الأمريكية والتكالب أتى بصورة متتالية حول الإسلام "ما يؤكده أكبر احمد عالم الانتربلوجيا الذي يرى أن الإسلام تحت الحصار وهو حصار تفرضه رؤى سياسية واستراتيجية وإعلامية إيديولوجية عامة معادية للإسلام ويعيب على دارسي الإسلام

خاصة بعد 11 سبتمبر 2001 نزعتهم الانتقائية في قراءة الإسلام وخاصة في حقل الإعلام ويقول أن خبراء الإعلام جاهزين على الفور كلهم مذنبون في مثل هذا الاستخدام الانتقائي للإسلام عموما وللقران الكريم لتدعيم وجهات نظرهم الجاهزة ويؤكد كذلك على أن رؤية العامة للإسلام تتسم برؤية تبسيطية تحصر الإسلام بالعنف والإرهاب"[17] وهو أيضا نتيجة لتراكمات لن نقف عندها لكون الموضوع يتناول الجريمة الالكترونية التي تستهدف الإسلام من خلال المواقع الالكترونية والتي تعتبر ما ينشر فيها من باب حرية التعبير فأين تتوقف حرية التعبير لتصبح جريمة تهدد امة كاملة يتجاوز تعدادها مليار نسمة.

ج مواقع الإرهاب وصورة الإسلام: تنتشر عبر الانترنت المواقع الالكترونية الخاصة بالجماعات المتطرفة دينيا وعلى وجه الخصوص ما يعرف أو ما يصطلح عليه الجماعات الإرهابية الإسلامية أو كما تلقب بالجماعات الجهادية والغرض من الوقوف مطولا عند هذه النقطة هو محاولة ملامسة خطر مثل هذه المواقع والتي تعد من الجرائم الالكترونية ليس فقط بالنسبة للإسلام إنما أيضا للإنسانية ككل فالمعلومات التي تتعمد الجماعات تمريرها عبر الانترنت وخاصة على موقع يوتيوب يهدف بالأساس للتخويف والترهيب ومن جهة أخرى يعطينا معلومات مغلوطة عن الإسلام ويشوهه كدين سلم ومحبة ويضعه في مرتبة "الشر" الذي تجب مواجهته ومقاومته بشتى الطرق والأشكال، ومن خلال الفيديوهات المتداولة عبر هذه المواقع سواء الخاصة بها ؟ أو عبر يوتوب لاحظنا أن كل قيم الوحشية والحقد والكراهية الترهيب والتخويف موجودة فيها ونذكر على سبيل المثال الفيديو الذي يصور إعدام 21 مصري مسيحي من طرف جامعة متشددة تبرر أعمالها من خلال تقديم نفسها أنها جماعة إسلامية جهادية أو حتى الفيديو المتداول إلى غاية اليوم

والذي يصور إحراق الطيار الأردني الكساسبة والذي نجد كل مراحل حرقه في الفيديوهات إلى غاية اليوم ولم يتم حذفه من اليوتيوب رغم طلب أسر وعائلات الضحايا ذلك إلا أن كل الفيديوهات موجودة على الموقع وشوهد الفيديو الأول في رابط واحد أكثر 17160 مرة، والفيديو الثاني 3337463 مرة مع الإشارة أن كل من الفيديوهات يتم رفعها من الموقع من عشرات الروابط التي تستثمر في مثل هذه الصور والتسجيلات للكسب المالي بالإضافة لفضول المتلقي.

وبث هذه الفيديوهات والتي تعد من أساليب التشهير بالأعمال الإرهابية يعد من الجرائم الالكترونية الخطيرة جدا والتي تتجاوز الدول والحدود أيضا ولعل هذا أيضا من بين سلبيات الانترنت، ونفس الشيء يمكن أن يقال حول الفيديو المتداول باغتيال الفرنسي ...... والذي مازال على الانترنت هو الأخر وتمت مشاهدته أكثر من .... بعد أن بثته قناة تلفيزيونية خاصة.، مثل هذه الجرائم التي تمرر عبر مواقع عالمية تشوه الإسلام والمسلمين ولعل الحقد والكره الذي ناله الإسلام والمسلمين بعد 11 سبتمبر بغض النظر عن حيثياته وعن مدى تورط أسامة بن لادن فيه أو مجرد سيناريو أمريكي لاحتلال افغنستان والعراق وتقسيم الوطن العربي وجعل الإسلام العدو الأول للحضارة الغربية يصبح مبرر حين نشاهد انتشار فيديوهات القتل ووصايا التوعد بالقصاص وكذا باغتصاب النساء وجعلهن سبايا حرب وغيرها من هرج يبرر باسم الإسلام في حين أن الجانب المشرق من الإسلام لا يكاد يرى وإن كانت بعض المحاولات فإن الملاحظ عليها أنها محاولات أقل ما يقال عنها جاهلة خاصة ما لاحظنه من خلال الفيديوهات المتداولة عن الإسلام مثلا والتي نرى فيها داعية يرينا عظمة الإسلام في ديك ينطق حسبهم باسم الله حتى لا يذبح ولعل مثل هذه الفيديوهات تشوه الإسلام أكثر وتجعله يقدم على أنه

دين خرافات في حين نبتعد عن التفسيرات العلمية التي وإن وجدت إلا أنها غير كافية.

ويطرح للتساؤل هو كيفية بقاء هذه الفيديوهات والتي تعد من الجرائم الالكترونية في حين لا توجد جهة تمثل الإسلام تأسست كطرف مدني سواء في الجزائر أو غيرها لتحاكم وتمنعها أو على الأقل تحجبها عن الظهور، ففي الكثير من الأحيان يطلع عليها الأفراد من باب الفضول خاصة أن تداولت على التلفيزيونات ما يجعل الوسيلة الإعلامي طرف في الجرم أيضا لأنها تعيد عرض جريمة تعرض لها أشخاص وبأبشع الوسائل الممكنة وهنا تتداخل المهنية والحق في المعلومة مع القيم الإنسانية والإسلامية التي تتبنى الرحمة كل القيم الإنسانية الراقية.، ولا يجب أن نتعجب أن وصفنا وألان نحن المسلمين بالإرهاب فالصورة التي يراها المجتمع الدول هي صورة مظلمة بسبب هذه المواقع التي يمكن أن توصف بالهدامة لقيم الدين الإسلامي وصورة المسلم المنهكة منذ عقود.

ومن جهة أخرى فإن هذه المواقع هي من بين الأسباب التي تجعل الدين الإسلامي في قفص الاتهام بالنسبة لغير المسلمين وأيضا قد تكون مفتعلة لأغراض جيوسياسية حيث يبقى التأكد من مصدرها صعب جدا فمثل هذه الأساليب مطبقة باحترافية إذ "تدل الشواهد والدراسات الإحصائية على ازدهار أجهزة الاتصال الدولية التي تدعو إلى الرذيلة وتحمل دعاوى الشر وتثير العنصرية وتشعل الأحقاد بين الأمم والشعوب وتسهم في تدمير العلاقات بين بني الإنسان بفعل ما تزرعه من بذور الفتن وما تبثها من الحقد والكراهية منطلقة في ذلك من مفاهيم وعقائد ومذاهب منحرفة مستهدفة من وراء ذلك تحقيق مصالح سياسية ومكاسب اقتصادية معتمدة على ما تملكه من أجهزة حدية ووسائل الكترونية وتكنولوجيا متقدمة وما

نضعه من خطط علمية مستثمرة احدث معطيات العصر في علوم الاتصال وفنون السيطرة على الرأي العام وغسل الأدمغة وتكوين الاتجاهات المتوافقة مع فكرها وايديولوجيتها مستندة في ذلك إلى انعدام العدالة في ملكية مصادر المعلومات وفقدان السيطرة عليها وعدم توزيعها مما يؤدي إلى نقص المعلومات اللازمة عن الإسلام والمسلمين."[18] لتحل محلها المعلومة المغرضة التي تبث عبر مثل هذه الفيديوهات والمواقع في حين هي من الناحية القانونية تعد من بين أخطر أنواع الجرائم الالكترونية التي تدعو للقتل أو التي تصور التنكيل والتعذيب لأشخاص من طرف جماعات متعصبة الفكر أو مدفوعة الأجر.

ويمكن أن نؤكد من خلال تتبعنا أيضا لبعض المجموعات على الفايس بوك التي تقول أنها مجموعات تعلن أنها جزائرية تسعى أيضا لتشويه الدين الإسلامي من خلال التشكيك في الله وسب الذات اللاهية من خلال منشورات بعض الأعضاء في المجموعة وكذا نشر البلبلة حول الدين الإسلامي الرسول القرآن وفي كل ما له صلة بالإسلام لكن الملاحظ أن أصحاب هذه المنشورات يقومون أيضا بتعليقات مستفزة للحصول على ردود فعل عنيفة عادة ما تنتهي بالسب والشتم ولكن ليس لإدارة الفايس بوك التدخل في نوعية المضامين ما دامت لا تنم عن عنف أو فحش مباشر وتعتبر باقي المنشورات عبارة عن حرية تعبير ورأي ؟؟؟ ونضع نقاط استفهام لأن حتى الحرية بمفهومها الفلسفي لها حدود لا يمكن تجاوزها، والخطورة التي نشير لها هي من خلال العدد الكبير لمستخدمي الموقع فايس بوك إذ "قالت الدراسة التي أوردتها مجلة كمبيوتر **وورلد الأمريكية** على موقعها الالكتروني أن عدد مستخدمي شبكات التواصل الاجتماعي سوف يرتفع بحلول 2017 إلى 2,33 مليار شخص."[19] وهو المجتمع العالمي الافتراضي الذي يتجاوز أكبر دولة في

التعداد السكاني الصين فيمكن أن نتخيل التطور والتزايد الذي سيكون في مجال الجريمة الالكترونية.

د – حجاب الفتاة الجزائرية: تتعرض صورة الحجاب للكثير من الإساءة سواء للحجاب كلباس شرعي أو للفتاة التي تلبس هذا الحجاب بغض النظر عن ماهية الحجاب لكنه كمتغير يمثل الهوية الوطنية للدول الإسلامية إلا أن نشر مقاطع فاضحة تلصق بالحجاب أولا وبالفتاة الجزائرية ثانيا هو ما يعد جريمة في حد ذاتها يعاقب القانون عليها فهذا الازدراء الذي لمسناه من خلال المقطع الذي اطلعنا عليه يصور حسب ناشره المجهول والذي اكتفى بتسميه نفسه ميسوم بالرسوم المتحركة فتاة شبه عارية ترتدي بنطال وتقدم نفسها على أساس أنها جزائرية وتلبس الحجاب؟ والواقع أن الفيديو المصور والذي مدته دقيقة وثلاثة عشر ثانية ومعنون بالحجاب في الجزائر يعد تعدي ليس فقط على صورة الفتاة الجزائرية بل وعلى الإسلام في الجزائر ويبقى مجهول المصدر وهو حسب المختصين قد يدخل في إطار الحرب المعلوماتية والتي تجعل من بعض الدول وأجهزتها الاستخبارية تقوم بالجرائم الالكترونية والتي تمس في هذا الإطار الشرف والدين ويتم تداول الفيديو الآن عبر الهاتف النقال فهو الآخر واحد من ناشري الجريمة الالكترونية ولعل هذا الأخير يجعل من الصعب محاصرة مثل هذه الجرائم الالكترونية واسعة التداول بين الشباب خاصة وقد يعتبره خاصة الطبقة العامة أنه من بين المسلمات أو الصفات التي تلصق فيما بعد بالحجاب وبالفتاة الجزائرية فتكون صورة ذهنية سلبية عن الحجاب وعن الفتاة المسلمة في الجزائر أيضا وهو متواجد وغيرها من الفيديوهات على موقع اليوتيوب الذي "يزوره يوميا مليار زائر ... والإحصائيات تبين أن ما

يتم رفعه من الموقع خلال 60 يوم فقط يفوق مجموع ما أنتجته أشهر 3 شركات إنتاج أمريكية خلال 60 سنة."[20].

3 -الحياة الشخصية والحق في الصورة: التعرض للحياة الشخصية للأفراد يعد من بين الجرائم الكترونية وهو نتحدث عن الهوية الفردية للشخص والتي تصبح مهددة هي الأخرى من خلال مختلف أنواع الإساءة التي يتعرض لها الفرد من طرف المجرم الذي تكون له نية تشويه سمعة الفرد أو المؤسسة من خلال نشر الصور والفيديوهات التي تمس الشرف وكذا صورة المؤسسات السيادية في الدولة كبث عبر اليوتوب فيديوهات لعناصر الأمن الوطني وهو يرقصون أو لأفراد الجيش وقد لا يقدر مقدار التشويه الذي ينال مثل هذه المؤسسات السيادية من خلال الترويج لصورة في الواقع قد تمثل الفرد نفسه فقط ولكن الزي الرسمي الذي يرتديه الفرد يصبح محل جريمة أيضا وفي الواقع هناك العديد من هذه الفيديوهات متداولة عبر مواقع شبكة الانترنت، أما فيما يخص الحق في الصورة فيمكن أن نعرفها كما يلي "هو ذلك الاستئثار الذي يتيح للشخص منع غيره من أن يرسمه أو يلتقط له صورة دون إذن منه صريح أو ضمني وما يستتبع ذلك من حقه في الاعتراض على نشر صورته على الجمهور"[21] ويقوم الكثير من الأفراد عبر مواقع التواصل الاجتماعي بالاصطياد في هذه الشبكات الفرائس خاصة الأطفال والمراهقين ويغروهم بأساليب مختلفة ليتحصلوا على صورهم ومن ثمة يبتزوهم بطرق مختلفة عبر فضحهم مثلا في النت لو رفضوا الاستجابة لطلباتهم سواء المادية أو أخرى ويلاحظ أن هذا النوع من الجرائم ازداد خاصة مع انتشار استعمال شبكات التواصل الاجتماعي من طرف الأطفال والمراهقين ومن الملاحظ أيضا أن هذا النوع من الجرائم يسكت عنه في الكثير من الأحيان خوفا من العقاب

من طرف العائلة والمجتمع الذي لا يتقبل مثل هذه الجرائم وتدخل في خانه الممنوعات لذا يفضل الكثير من الضحايا الصمت والاكتفاء بتغير حساب الفايس بوك فقط وكذا رقم الهاتف" ولا يمكن حصر صور الاعتداء على حق الإنسان في صورته الشخصية ويعتمد ذلك على غاية المعتدي عليها فقد يكون بقصد استغلالها ماديا وقد يكون بهدف الإساءة لصاحبها للتأثير عليه في الانتخابات مثلا وقد يكون الدافع الانتقام ونذكر بعض الأمثلة حسب القانون عند أغلب الدول:

نشر معلومات وحقائق قد توثقها الصور الشخصية تكون محرجة للشخص ونجعله موضع ازدراء في نظر الناس.

نشر صور ضحايا الجريمة أثناء حالة الصدمة أو وهم تحت وطأة الجريمة خلافا لرغبتهم في عدم عرض مأساتهم وهلعهم من هول الجريمة على الناس مع نعذر الناشر بمبدأ الحق في الإعلام.

نشر الصورة دون الاسم مع كتابه عبارات تحتها تثير السخرية والاستهزاء بصاحب الصورة."[22].

ويمكن أن تصنف هذه الجرائم في خانة التجسس على الغير عبر ولوج المعتدي إلى وثائق خصوصية عبر الانترنت ومن ثم نشرها للعامة كالصور العائلية مثلا أو حتى صور الأعراس ونتأسف لكون مثل هذه الأخيرة موجود بصورة كبيرة دون علم أصحابها والعائلات أنها تعرضت لجريمة الكترونية ينقل تفاصيل حياتهم الخاصة إلى الانترنت ومنها إلى الهاتف النقال الذي ازدهرت سوقها في الجزائر خاصة في العقد الأخير وهذا الحق في الخصوصية لا يحترم وكما يعرفها **الاهواني** "فهي حق الإنسان في أن نتركه يعيش وحده بحيث يخلو إلى نفسه وأن يختلي بالناس الذين يألفهم وذلك من أدنى حد للتدخل من جانب الغير ويتمثل ذلك أساسا

في أن يكون بعيدا عن تجسس الغير وأعينهم ولا يجوز نشر ما يمكن أن يتم العلم بد دون تجسس فالعلم بالخصوصيات لا يبرر نشرها دون إذن من صاحب الشأن"[23]، وهذا التعدي على الخصوصية ونشر التفاصيل الشخصية لها بعد عالمي حيث "قدّرت التقارير الأخيرة حجم المبالغ التي يجنيها لصوص الإنترنت بنحو 160 مليار دولار سنويا، بمعدل 48 ألف دولار شهريا. يجد لصوص الانترنت في مواقع التواصل الاجتماعي فرصة ذهبية لتحقيق أموال طائلة، حيث تزخر شبكات مثل «فيسبوك»، «تويتر»، و«غوغل» بملايين البيانات الشخصية والصور للمشتركين، ولأن البيانات الشخصية أصبحت العملة الرائجة اليوم في الأسواق الرقمية، ومثلها مثل أي عملة، فإنها تحتاج إلى وجود أجواء من الاستقرار والثقة عبر إصدار تشريعات وقوانين لحماية البيانات الشخصية من عمليات الاختراق والسرقة التي تتعرض لها بصورة كبيرة حاليا."[24].

5 – واقع الجريمة الالكترونية في الجزائر وإمكانية التصدي لها على أرض الواقع: إن محاصرة الظاهرة الاجتماعية صعب جدا على أرض الواقع نظرا للاختلافات التي تميز مجتمعات الدراسة وهو ما ينطبق على الدراسات التي يكون الواقع نسقا لها ومن الأكيد أن ضبط ودراسة الجريمة الكترونية هو من الصعوبة ما كان وهذا نظرا لكون المجتمع افتراضي صعب التحديد وهذا النوع من الجرائم يصعب ضبطه من الناحية القانونية أيضا لكن هناك مبادرات عبر العالم للإحاطة بها والتحكم فيها وفرض قوانين تعاقي مرتكبيها، "احتلت الجزائر بناءً على التقارير الأخيرة المراتب الأولى إفريقيا وعربيا بنسبة 85 بالمائة في القرصنة والجريمة الإلكترونية، ما جعلها الجزائر من بين أبرز عينات واهتمامات تقارير المنظمات والهيئات الدولية المختصة.، وكانت الجزائر ضمن مجموعة الدول المدرجة في

مشروع إعداد بحث لتحديد آلية تطور الهجمات الإلكترونية خلال السنوات الثمانية المقبلة، من طرف منظمة «التحالف الدولي لحماية أمن الأنترنت»، الذي يتضمن تقديم إرشادات لحكومات الدول والسلطات المحلية حول أفضل السبل المتاحة لمواجهة هذه الهجمات."[25]، وفي الواقع الجزائري هناك قوانين شرعت لمحاربة الجريمة الالكترونية ولكنها لا تتضمن قوانين حول المس بالهوية الوطنية كالدين مثلا تبقى القوانين التي يجتهد فيها فقهاء القانون غير كاملة وهذا نظرا لكون هذه الجريمة تتطور كل يوما ومن الصعب مواكبتها في شتى التفاصيل التي تمسها.

كما تسعى الجزائر من خلال الأجهزة التي تمتلكها أن تحاصر وتحارب هذا الواقع وكالدرك الوطني وجهاز الأمن الوطني الذي يسعى للتصدي لهذا النوع من الجرائم "فاثر تفاقم ظاهرة استخدام التكنولوجيا في مختلف أشكال الإجرام تم سنة 2007 تدعيم مخابر الشرطة العلمية والتقنية بأقسام مختصة في الأدلة الرقمية على مستوى المخابر الثلاث المتواجدة بكل من العاصمة وهران قسنطينة تكمن مهامها في استغلال الأجهزة الالكترونية التي يشتبه استعمالها في ارتكاب الجرائم وذلك بهدف استخراج المعطيات المخزنة بداخلها والتي من شانها أن تساعد المحققين في التحقيق وتلك التي تشكل في حد ذاتها أدلة إقناع."[26]، وأما الناحية القانونية فإن الحقوقي **قسنطيني** يرى أن تطبيق التشريع على أرض الواقع صعب جدا إن «استصدار الجزائر قوانين لمعاقبة مرتكبي الجرائم الإلكترونية غير كاف، مع عدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وحدّة أضرارها قبل إصدار العقوبة، هذا فضلا عن غياب التواصل الدائم بين القضاء والمختصين في الاتصالات، ما أفرز شبه تذبذب وغموض في شأن العقوبات الدقيقة في مثل هذه الجرائم». في السياق ذاته أوضح محدثنا أن القانون الجزائري، يعاقب في الغالب

مرتكبي هذه الجرائم بالسجن القصير المدى أو بالغرامة المالية، «بحكم أن جل الجرائم الإلكترونية المرتكبة في الجزائر تصب أو تصنّف قانونيا كسرقة»، مبرزا أن المعدل العام لهذه الجرائم في الجزائر متوسط مقارنة بباقي دول العالم، محذّرا من تنامي هذه الجرائم في السنوات الأخيرة على المستوى الوطني"[27]. بالإضافة لأسباب أخرى يمكن أن نذكر منها وحسب عميد مصطفى عبد القادر[28]:

1 – في حالة ارتكاب الجريمة انطلاقا من الجزائر ومن طرف جزائريين وكانت آثارها خارج الوطن نعتمد على الأدلة التي يمكن تحصيلها من محيط المشتبه فيه بسبب صعوبة تحصيل الأدلة من موقع ظهوره الجريمة بالخارج.

2 – عملية تحصيل معطيات الارتباط لدى مزودي الانترنت تتطلب وقت طويل نظرا لتمركزها بالعاصمة.

عدول الضحايا عن الإبلاغ عن الجرائم التي يتعرضون لها إما بسبب جهلهم أن القانون يجرم تلك الأفعال ويحميهم وإما خشية من ردود أفعال محيطهم خاصة بالنسبة للمؤسسات التجارية كالبنوك أو الأشخاص الطبيعيين لما يتعلق الأمر بقضايا ماسة بالآداب.

الخاتمة: بعد استعراضنا لكل هذه المعطيات يمكن أن نستنتج أن الجريمة الالكترونية تمس كل المجتمعات عبر العالم بعد ان تكونت مجتمعات افتراضية تحول الكمبيوتر والوسائل الأخرى الحديثة للاتصال لمسرح للجريمة فباتت جريمة كاملة الأركان ونتائجها المادية ضخمة جدا عبر العالم لكن أثارها على الأمم يتجاوز الجانب المادي إلى العقائدي والفكري خاصة الإسلام الذي يتعرض لمختلف أنواع التشويه والإساءة في ظل معطيات دولية وقومية تفرض الحفاظ على مقومات الهوية الوطنية لكل أمة بالإضافة لضعف القاعدة القانونية التي تعتبر غير كافية

للحد ومحاصرة ومعاقبة هذا النوع من الجرائم رغم كل الجهود التي تبذل علة المستوى العالمي وليس فقط على مستوى الجزائر، ليبقى الصراع بين الخير والشر قائم في ظل معطيات عالمية تشير إلى تزايده في السنوات القادمة إلى أضعاف ما هي عليه الآن.

المراجع باللغة العربية:

الكتب:

1- أحمد محمد صالح، **الانترنت والمعلومات، بين الأغنياء والفقراء**، مركز البحوث العربية والإفريقية، 2000، دط.

2 - ادوارد كولد سميث، جيري مانديرـ ترجمة: رجب بو دبوس، **محاكمة العولمة**، المركز العالمي لدراسات وأبحاث الكتاب الأخضر، دط، ليبيا، دون سنة.

3 - محي الدين عبد الجليل، **الدعوة الإسلامية والإعلام الدولي**، دار الإشعاع مصر، دط، دسنة .

4 - عبد الرزاق الدليمي، **صناعة الإعلام العالمي المعاصر**، اليازوري، عمان الطبعة الأولى، 2015.

الأطروحات والمذكرات:

5- باسل عبد المحسن القاضي، **تداول المعلومات عبر الانترنت وأثره في تشكيل الوعي في عصر العولمة**، الأكاديمية العربية المفتوحة في الدانمارك، دولة الدانمارك، 2007، ص 17.

6 - يوسف صغير، **الجريمة المرتكبة عبر الانترنت**، مذكرة ماجيستير في القانون، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

7- سعيدي عبد القادر حسن، **الجريمة الالكترونية في الجزائر مواطنين ومؤسسات جزائرية أمام الجريمة الالكترونية**، مذكرة ماستر في الصحافة العلمية المدرسة الوطنية العليا للصحافة وعلوم الإعلام، الجزائر، 2014.

المجلات:

8 – عبد العزيز غرمول، **هل ينتخب رئيسا بالوكالة لعالم الغد، النفوذ اللامرئي لأميركا**، مجلة عالم السياسة، العدد الثالث، 1992، الجزائر.

9 – محمود الفطافطة، **الإعلام الجديد ...رقابة ناعمة وحرية بلا قيود**، مجلة تسامح، مركز رام الله للدراسات وحقوق الإنسان، العدد 34، فلسطين، 2011،.

10 – ياحي احمد، **الجريمة الالكترونية**، مجلة الشرطة، عدد 120، الجزائر 2013.

11 – فيصل الحفيان، **اللغة والهوية، إشكاليات المفاهيم وجدل العلاقات**، مجلة التسامح، عمان، 2004.

12 – احمد صدقي الدجاني، **الحوار مع الأخر**، مجلة **التسامح:** عدد 2، عمان 2003.

13 – فيصل دراج، **المثاقفة بين الرغبة والحقيقة**، مجلة **التسامح**، عدد 2 2003.

14 – سميرة على أبو غزالة، **أزمة الهوية ومعنى الحياة كمؤشر للحاجة إلى الإرشاد النفسي**، معهد الدراسات التربوية، مصر، د سنة.

15 – معتز الخطيب، **ظاهرة كراهية الإسلام، الجذور والحلول**، مجلة ثقافتنا للدراسات والبحوث، المجلد 5، العدد 17، 2008، قطر.

16 – حسن السويداني، **تكنولوجيا الإعلام الجديد وانتهاك حق الخصوصية** مجلة دفاتر السياسة والقانون، العدد 11، 2014.

17 – فهيد محسن الديحاني، **الطبيعة القانونية للحق في الصورة الشخصية وحمايتها المدنية في القانون الكويتي**، المجلة العربية للدراسات الأمنية والتدريب المجلد 28 العدد 52، دط، دسنة.

الجرائد:

18 – قاسمي أ، **160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الانترنت، قسنطيني: تطبيق العقوبات في قضايا الجريمة الالكترونية صعب جدا في الجزائر**، جريدة اللام اليوم اون لاين، عدد 24.1.2014. شوهد في 10.08.20115/ الساعة : 14:00.

الملتقيات:

19 – مصطفى عبد القادر، **الشرطة الوطنية ومكافحة الجريمة الالكترونية** ملتقى دولي الجزائر، محاربة الجريمة الالكترونية 2010، الجزائر.

الهـــوامش:

1- احمد محمد صالح، **الانترنت والمعلومات، بين الأغنياء والفقراء**، مركز البحوث العربية والإفريقية، 2000، دط، ص 55.

2- باسل عبد المحسن القاضي، **تداول المعلومات عبر الانترنت وأثره في تشكيل الوعي في عصر العولمة**، الأكاديمية العربية المفتوحة في الدانمارك، دولة الدانمارك، 2007، ص 17.

3- عبد العزيز غرمول، **هل ينتخب رئيسا بالوكالة لعالم الغد، النفوذ اللامرئي لأميركا**، مجلة عالم السياسة، العدد الثالث، 1992، الجزائر، ص 57.

4- محمود الفطافطة، **الإعلام الجديد ...رقابة ناعمة وحرية بلا قيود**، مجلة تسامح، مركز رام الله للدراسات وحقوق الإنسان، العدد 34، فلسطين، 2011، ص

5- يوسف صغير، **الجريمة المرتكبة عبر الانترنت**، مذكرة ماجيستير في القانون، جامعة مولود معمري، تيزي وزو، الجزائر، 2013،ص 09.

6 - نفس المرجع السابق، ص، نفس المكان.

7 - ياحي احمد، **الجريمة الالكترونية**، مجلة الشرطة، الجزائر، عدد 120، 2013، ص 89.

8 - نفس المرجع السابق، نفس المكان.

9- سعيدي عبد القادر حسن، **الجريمة الالكترونية في الجزائر مواطنين ومؤسسات جزائرية أمام** الجريمة الالكترونية، مذكرة ماستر في الصحافة العلمية، المدرسة الوطنية العليا للصحافة وعلوم الإعلام، الجزائر، 2014، .ص 26،27. بتصرف وترجمة من الباحث.

10- مجلة **التسامح:** احمد صدقي الدجاني، **الحوار مع الأخر**، عدد 2، عمان، 2003، ص 17.

11- ادوارد كولد سميث، جيري مانديز، ترجمة: رجب بو دبوس، **محاكمة العولمة**، المركز العالمي لدراسات وأبحاث الكتاب الأخضر، دط، ليبيا، دون سنة، ص 19.

12- فيصل دراج، **المثاقفة بين الرغبة والحقيقة**، مجلة **التسامح:** مرجع سبق ذكره ص 50.

13- فيصل دراج، مرجع نفسه نفس المكان.

14 - فيصل الحفيان، **اللغة والهوية، إشكاليات المفاهيم وجدل العلاقات**، مجلة التسامح، عمان 2004، ص39.

15 - سميرة على أبو غزالة، **أزمة الهوية ومعنى الحياة كمؤشر للحاجة إلى الإرشاد النفسي** معهد الدراسات التربوية، مصر، د سنة، ص 261.

16 - فيصل الحفيان، **اللغة والهوية، إشكاليات المفاهيم وجدل العلاقات**، مرجع سبق ذكره، ص 46.47.

17 - معتز الخطيب، **ظاهرة كراهية الإسلام، الجذور والحلول**، مجلـــة ثقافتنا للدراسات والبحوث، المجلد 5، العدد 17، 2008، قطر، ص 61.

18 - محي الدين عبد الجليل، **الدعوة الإسلامية والإعلام الدولي**، دار الإشعاع، مصر، دط دسنة، ص **17**.

19 – عبد الرزاق الدليمي، **صناعة الإعلام العالمي المعاصر**، اليازوري، عمان، الطبعة الأولى 2015، ص 127.

20 – نفس المرجع السابق، ص 126.

21 – فهيد محسن الديحاني، **الطبيعة القانونية للحق في الصورة الشخصية وحمايتها المدنية في القانون الكويتي،** المجلة العربية للدراسات الأمنية والتدريب، المجلـــد 28 العدد 52، دط دسنة، ص 204.

22 – نفس المرجع السابق، ص. 204. 205.

23 – حسن السويداني، **تكنولوجيا الإعلام الجديد وانتهاك حق الخصوصية**، مجلة دفاتر السياسة والقانون، العدد 11 ،2014،ص 220.

24 – قاسمي أ، **160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الانترنت قسنطيني: تطبيق العقوبات في قضايا الجريمة الالكترونية صعب جدا في الجزائر**، جريدة اللام اليوم اون لاين، عدد 24.1.2014. شوهد في 10.08.20115/ الساعة:14:00 مرة واحدة.

25 – نفس المرجع السابق.

26 – مصطفى عبد القادر، **الشرطة الوطنية ومكافحة الجريمة الالكترونية**، ملتقى دولي الجزائر محاربة الجريمة الالكترونية 2010، الجزائر، ص 125.

27 – قاسمي أ، **160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الانترنت قسنطيني: تطبيق العقوبات في قضايا الجريمة الالكترونية صعب جدا في الجزائر، مرجع سبق ذكره.**

28 – مصطفى عبد القادر، مرجع سبق ذكره، ص 130.

واقع الملكية الفكرية في عصر التسارع الرقمي

د. محمد يونسي

المركز الجامعي الونشريسي، تيسمسيلت

بسم الله الرحمن الرحيم والصلاة والسلام على أشرف خلق الله أجمعين سيدنا محمد الأمين وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين.

أمّا بعد:

تروم هذه الورقة البحثية الوقوف على قضية محورية ومهمّة في أخلاقيات البحث العلمي والمعرفي في شتى التخصّصات والفروع علمية كانت أم أدبية وفنية ألا وهي: واقع الملكية الفكرية في عصر التسارع الرقمي.

نشأة الملكية الفكرية: ممّا لا شكّ فيه أنّ الطبيعة الإنسانية جبلت على حبّ التملّك، على اعتبار تمسّك الإنسان بكلّ ما نتج عن إبداعه العقلي وكلّ ما يمتّ بصلة لإنتاجه الفكري، فقد تزامنت هذه الطبيعة والملكية الفكرية، وتجدر الإشارة إلى وجود سبق للإنتاج الفكري قبل صدور القوانين التي تحميه[1].

فالملكية الفكرية وبراءة الاختراع ...، تسميات تصبّ في حقل واحد حيث لا يحقّ لأيّ شخص أو هيئة التطاول عليها دون إذن خطيّ أو تصريح علني أو موافقة من صاحب العمل الإبداعي أو الاختراعي، لهذا سعت دول العالم لسنّ قوانين تكفل هذا الحقّ، وتحديدا في عصرنا الحالي الذي واكب ما يعرف بالتسارع التكنولوجي، حيث استحال العالم بأسره قرية صغيرة لا حدود لها، إنّه العصر الذي سيطرت فيه التقنية على التفكير البشري، عصر أزاح الحواجز وألغى التأشيرة فأصبح الواحد منّا يتجوّل بحريّة في فضاء افتراضي هو في حقيقة الأمر امتداد للعالم الملموس.

وتتبادر إلى الأذهان لأول وهلة مجموعة من التساؤلات لا بد أن نبحث لها عن إجابات أو مقترحات وهي :

- هل يوجد في العالم العربي حضور للملكية الفكرية ؟ .
- ما مصيرها في عصر التسارع الرقمي ؟ .

لقد فطن الكّتاب والمؤلفون العرب مبكرا لمسألة حماية ملكيتهم الفكرية وكتاباتهم الأدبية والإبداعية، ونقرأ للمؤرخ العربي الكبير **أبو الحسن المسعودي**[2] صاحب كتاب "**مروج الذهب**" المتوفى سنة **346هـ** وهو يقول عن كتابه:

« فَمَنْ حَرَّفَ شَيْئًا مِنْ مَعنَاهُ، أو أَزَالَ رُكْناً مَنْ مَبْنَاهُ، أو طَمَسَ وَاضِحَةً مِنْ مَعَالِمِهِ، أو لَبَّسَ شَاهِدةً مِنْ تَرَاجُمِهِ، أو غيّره، أو بدّله، أو أَشَأَنَهُ، أو اخْتَصَرَهُ، أو نَسَبَهُ إلى غَيْرِنَا أو أَضَافَهُ إلى سِوَانَا، فَوَافَاهُ مِنْ غَضَبِ الله وَسُرْعَةِ نِقَمَهِ وَفَوَادِحِ بَلاَيَاهُ مَا يَعْجَزُ عَنْهُ صَبْرُهُ، وَيَحَارُ لَهُ فِكْرُهُ، وَجَعَلَهُ اللهُ مُثْلَةً لِلْعَالَمِينَ، وَعِبْرَةً لِلْمُعْتَبِرِينَ، وَآيَةً لِلْمُتَوَسِّمِينَ، وَسَلَبَهُ اللهُ مَا أَعْطَاهُ، وَحَالَ بَيْنَهُ وَبَيْنَ مَا أَنْعَمَ بِهِ عَلَيْهِ: مِنْ قُوَّةٍ وَنِعْمَةِ مبدع السموات والأرض، مِنْ أَيِّ المِلَلِ كَانَ والآرَاءِ، إنَّهُ عَلَى كُلِّ شَيْءٍ قَدِير، وقَدْ جَعَلْتُ هَذَا التَّخْوِيفَ فِي أَوَّلِ كِتَابِي هَذَا وَآخِرَهُ، ليكون رادعا لمن ميله الهوى أو غلبه شقاء فَلْيُرَاقِبْ أَمْرَ رَبِّهِ وَلْيُحَاذِرْ مُنْقَلَبَهُ، فَالمُدَّةُ يَسِيرَةٌ والمَسَافَةُ قَصِيرَةٌ وإلى الله المصير»[3].

وما ذكر من سرقة الكتب هو الدافع الأكبر الذي حدا **بالمسعودي** إلى أن يعلن في كتابه مروج الذهب الحرب على هؤلاء المتشبعين بما لم يعطوا، فقد اضطر إلى استهلال وختم كتابه بالتحذير .

لعلّ الحديث عن واقع الملكية الفكرية يهمّ الباحثين والمؤلفين كغيرهم من الناس حيث إنّهم يقضون ساعات طويلة في البحث والتنقيب والتفتيش عن قضايا ما تزال غامضة، وتحتاج شيئا من الشرح والتفسير والتحليل، الأمر يبدو عاديا إلى حدّ

الآن، لكن عندما ينشر هذا العمل الذي تطلّب جهدا وعناء كبيرين، في شكل مقال أو كتاب أو مؤلف من المؤلفات، هنا يستدعي الأمر شيئا مهمّا يسمّى حقّ الملكية الفكرية.

مفهومها وتأصيلها قانونيا:

مصطلح ملكية **PROPERTY** من الأصل **اللاتيني PROPRUIS** ويعني حقّ المالك أي حقوق الإنسان فيما يتعلّق بثمرة فكره، وكذلك كلمة فكري: فهي من اللاتينية **INTELLECTUALS** وتعني أيضا غير مادي وكل ما له علاقة بالجانب المعنوي في استقلاليته عن أي دعم مادي[4] .

أما الحقّ الفكري **INTELLECTUAL RIGHT** عبارة تعني الملكيات غير المادية وموضوعها فكري بحت.

والملكية الفكرية **INTELLECTUAL PROPERTY** تعبير عامّ يضمّ مجموع الملكيات الأدبيّة والفنيّة والملكية الصناعيّة وهي ما لا يتعلّق بتحقيق عملٍ وإنّما بتصوّره بخلاف مادي[5]".

هذه الملكية الفكرية تستلزم ما يعرف بحماية الملكية الفكرية، ويتلخّص جوهر الملكية الفكرية في أنّها تمنح الفرد حقّ الحماية للعمل الذي ابتكره أو أبدعه في مجال ما من مجالات الحياة، وتمكّنه من التصرّف دون غيره إلا بإذن خطي كما هو متعارف عليه دوليا في حقوق الملكية الفكرية، حيث تسهر الدول على صيانة هذا الحقّ من خلال سنّ قوانين ترمي إلى معاقبة كل من يعتدي على الملكية الفكرية لعمل ما مهما كان نوعه[6].

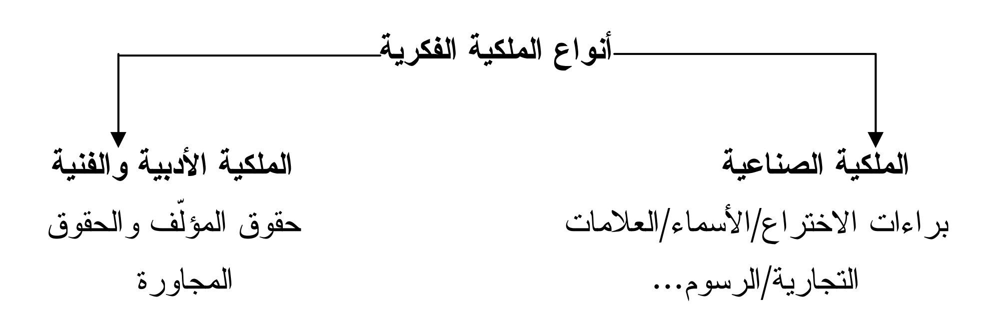
أما حق الملكية فإنّه حقّ طبيعي يقوم على العمل ومقدار العمل، لا على الحيازة أو القانون الوضعي، وليس لأحد حق فيما يكسبه المرء بتعبه ومهارته، ولا تصير الحيازة حقا إلا إذا استلزمت العمل، على أنّ حقّ الملكية خاضعٌ لشرطين:

- الأول: أنّ الملك لا يدع ملكيته تتلف أو تهلك.
- الثاني: أنْ يدع للآخرين ما يكفيهم فإنّ هذا حقٌّ لهم[7].

أنواع الملكية الفكرية: الملكية الفكرية نوعان:

1. **الملكية الصناعية:** وتشمل ما ينتجه العقل البشري في حقل العلوم والتقنية على سبيل: براءات الاختراع، العلامات التجارية (العبارات الإشهارية– الصور– الرموز– الدمغات–الرسوم) النماذج الصناعية ...
2. **الملكية الأدبية والفنية:** تختصّ بحق المؤلّف وتضمّ المصنفات الأدبية والفنية، من قبيل الروايات والقصائد والمسرحيات والأفلام والألحان الموسيقية واللوحات والصور الشمسية والتماثيل...[8]

وعليه نمثّل لأنواع للملكية الفكرية بالرسم الموالي:



المصنفات الرقمية المحمية على الشبكة العنكبوتية: يعدّ المصنّف الرقمي أحد إفرازات التكنولوجيا الحديثة، حيث إنّه لا يختلف في المسمى عن المصنّفات التقليدية ممثّلة في الكتب والقطع الموسيقية واللوحات الزيتية، وممّا لا يغرب على أيّ باحث متخصّص في هذا الميدان أنّ الاختلاف في الحامل، فقد حلّ الحامل الرقمي محلّ الحامل الورقي، ولهذا السبب أطلق عليها اسم المصنفات الرقمية[9].

يمكن القول إنّ المصنّف الرقمي هو مصنّف إبداعي يتحكّم فيه العقل البشري ولا يخرج عن الدائرة التي رسمها له وهي دائرة تقنية المعلومات والتي تستدعي معرفة واسعة وتحكّما جيّدا في التكنولوجيا الحديثة.

توجد على الشبكة الرقمية العالمية العديد من المصنفات الرقمية المختلفة، أمّا التي يحميها القانون بموجب حقوق المؤلف فهي: الملفات الرقمية لمصادر المعلومات، التقليدية نحو الكتب الرقمية والدوريات والموسوعات المتاحة عبر الشبكة العنكبوتية في شكل حديث رقمي، وهناك مصنفات محميّة بموجب قوانين الملكية الصناعية والتجارية على سبيل: البرمجيات وبرامج الحاسوب وقواعد البيانات، الدوائر المتكاملة أضف إلى ذلك الملفات الرقمية لمصادر المعلومات التقليدية من الكتب الرقمية والدوريات والموسوعات وما شاكلها من الملفات المتاحة عبر الشبكة والتي انتسبت إلى العالم الرقمي.

معظم من يحصل على نسخ مصورة أو منسوخة هو في الأساس لن يكون قادرا على دفع ثمن النسخة الأصلية إذا لم يحصل على تلك المسماة "**مقرصنة**" وبالتالي ففي كلتا الحالتين لا يعتبر زبونا حقيقيا، ومن جهة القائمين على حماية الملكية الفكرية تعدّ هذه التصرفات انتهاكــا لحقــوق مكتسبــة يكفلها القــانون، ممّا يتسببّ – على حدّ تعبيرهم – في خسائر ماديّة وقتل روح الاختراع والإبداع في الإنسان.

شواهد تثبت حضور الملكية الفكرية في الوطن العربي: يبدو أن ّ حماية الملكية قد تجسدت واستقرت فعلا في جميع الميادين قديما في مختلف النظم القانونية سواء أكانت إجرائية أم موضوعية، باستثناء الملكية التي تتعلق بالجانب الفكري مع العلم أنها تشكّل محورا هامّا تبنى عليه جلّ النتائج المتوصّل إليها في عالم الصناعات والاختراعات.

يعتبر الشخص مؤلِّفاً إذا نشر المصنّف المبتكر منسوباً إليه سواء بذكر اسمه على المصنف أو بأيّ طريقة أخرى ما لم يقم دليل على نفيه، وهذه النسبة لا يسوغ لصاحبها التنازل عنها لينتحلها شخص آخر، فكما لا يجوز التنازل عن الإنتاج الذري كذلك لا يجوز التنازل عن الإنتاج العلمي الذي هو نتاج العقول، ومن لطيف حفاوة العلماء بمؤلفاتهم أنهم جعلوها بمنزلة أعلى وأغلى من نسل أصلابهم حتّى قال بعضهم فيها:

مَا نَسْلُ قَلْبِي كَنَسْلِ صُلْبِي ★★★ مَنْ قَاس رُدَّ لَهُ قِيَاسُهْ

(أي رد له قياسه في المحبة) ولهذا فمن حقه الأدبي فيها أيضاً لا يصحّ التنازل عنه لأي جهة حكومية أو غيرها فرداً أو غير فرد بل تبقى له صفته الأدبية في التأليف[10].

بالنسبة **لجمهورية مصر العربية** أرست الجمعية المصرية للانترنت مجموعة من القواعد الأخلاقية ضمن ميثاق شرف.

وبالعراق تمّ تشكيل لجنة مزدوجة تضمّ كلاًّ من وزارتي الداخلية ووزارة العدل، وهي الوزارات التي تمتلك حقّ سنّ نصوص عقابية لجرائم الانترنت، وبناءً على توصيات المؤتمر الأمني العربي الذي شدّد على ضرورة وضع هذه النصوص العقابية قيد التنفيذ، وكان الهدف الأساس تجريم إساءة استخدام الانترنت وفرض عقوبات صارمة ضدّ كلّ من تسوّل له نفسه الاعتداء على أي حقّ – مهما كان نوعه – سار تحت غطاء قانوني[11].

أمّا **الحكومة التونسية** فقد وضعت قوانين كثيرة تنظّم استخدام الانترنت وحرصت على ألاّ يفلت قطاع الاتصالات من القوانين التي فرضتها الحكومة التونسية.

ولم تفرض الدول الآتية: **الجزائر** ولا **المغرب** ولا **فلسطين** أيّة قوانين لمراقبة محتويات الاتصالات عبر الانترنت، إنما اكتفت بإجراء تعديلات طفيفة على القوانين التي تسيّر حقوق المؤلّف وكذا الحقوق المجاورة، سعيا منها لمواكبة التغيرات التي تتماشى مع النشر الالكتروني[12].

تبدو الدول العربية أقلّ حضورا وأقلّ اهتماما بقضية حماية الملكية الفكرية ونلمس ذلك من خلال تماطلها في تطبيق حيثياتها وعدم حرصها على التماشي وما تفرضه الاتفاقيات الدولية.

الاعتداء على الملكية الفكرية وحقّ المؤلف على شبكة الانترنت: تشتمل حماية النشر الالكتروني على حماية حقّ الناشر في النشر بالدرجة الأولى، وحقّ المؤلّف في أن ينشر له ما يكتب... وبهذا الطرح تكون حماية حقوق الملكية الفكرية جامعة بين النشر والتأليف[13]، وإذا كان النشر الورقي يعتمد على الكتب والمنشورات المطبوعة، فإنّ النشر الالكتروني مادّته الخام المعلومات والبيانات الرقمية.

لقد أصبح حقّ التأليف من القضايا الشائكة بعد أن أضحى نشر أو نسخ أي مؤلّف أسهل الأمور لدى أي شخص يحسن التعامل مع الأساليب التكنولوجية الحديثة وبطبيعة الحال دون أدنى احترام للقوانين الخاصة بحقوق المؤلّف والتأليف ويعزى السبب لارتباط حقوق المؤلّف بالنسخة الورقية وغيابها في النسخة الالكترونية التي تتداول عبر الشبكة العنكبوتية، وبالتالي فمعظم قوانين حماية حقوق المؤلّف لا تطبّق على المواد المنشورة الكترونيا[14].

إنّ نشر المؤلّفات – مهما كان نوعها – الكترونيا في ظلّ غياب قوانين تحمي النشر الالكتروني يعني المخاطرة بها وبأصولها الإبداعية، ومن هنا فالعمل الإبداعي مهدّد ضمن هذه التقنية الجديدة التي وفدت إلينا في العصر الحالي، على اعتبار النشر الالكتروني أحد تحديات القرن الواحد والعشرين الذي يتيح الحرية

الكاملة للنفاذ إلى قواعد البيانات التي تحوي الآلاف من المنشورات الالكترونية الأدبية منها والعلمية[15].

ولا تخرج قواعد البيانات عن بقية موضوعات الملكية الفكرية من حيث أهمية إيجاد حماية قانونية لواضعيها والمستثمرين فيها فهي تسهم في تنمية المجتمع وسوق العمل، وتطوير قاعدة الفهم البشري وتوسيع المدارك في زمن تتسع فيه المعرفة كضرورة حتمية في سوق العمل، وعرض المهارات وتداول الإبداع وبناء روح المنافسة، إضافة إلى تسهيل عملية ولوج الباحثين إلى المواد البحثية، وتشجّع على الاستثمار في البحوث عالية الكفاءة، فضلاً عن إتاحة الفرصة للعامة لتفحص النتاج الأدبي والعلمي والبحثي.[16]

خاتمة: يرى الخبراء والمهتمون في هذا الحقل الذي يجمع بين ما هو فكري وما هو تقني، أنّ قوانين النشر لم تعد ردعا على المنشورات الالكترونية بحكم عمومية هذه الأخيرة، حيث يستطيع أيّ شخص الوصول إليها بحرية تامة ودون مقابل، ويتجاوز الأمر أحيانا حتى عدم التعرّض للمساءلة القانونية، مع العلم أنّ دخول الشبكة المعلوماتية أصبح حاجة ملحّة تقاس بها درجة تطور المجتمعات.

في الختام نقول ولسان حالنا قول الأولين: "**إنَّ مِنْ بَرَكَةِ العِلْمِ أَنْ تَعْزُوهُ لِقَائِلِهِ**".

الهوامش:

1 – ينظر: أبو اليزيد علي، حقوق المؤلّف الأدبية، مكتبة النهضة المصرية، القاهرة، ط/1 1999، ص: 31 .

2 – المسعودي علي بن الحسين بن علي، أبو الحسن المسعودي، من ذرية عبد الله بن مسعود: مؤرخ، رحالة، بحاثة، من أهل بغداد. أقام بمصر وتوفي فيها قال الذهبي: «عداده في أهل بغداد نزل مصر مدة، وكان معتزليا» من تصانيفه «مروج الذهب – ط» و«أخبار الزمان ومن أباده الحدثان» تاريخ في نحو ثلاثين مجلدا، بقي منه الجزء الأول مخطوطا [ثم طُبع] و«التنبيه والإشراف – ط» و«أخبار الخوارج» و«ذخائر العلوم وما كان في سالف الدهور» و«الرسائل»

و«الاستذكار بما مر في سالف الأعصار» و«أخبار الأمم من العرب والعجم» و«خزائن الملوك وسر العالمين» و«المقالات في أصول الدينات» و«البيان» في أسماء الأئمة و«المسائل والعلل في المذاهب والملل» و«الإبانة عن أصول الديانة» و«سر الحياة» و«الاستبصار» في الإمامة و«السياحة المدينة» في السياسة والاجتماع، وهو غير المسعودي الفقيه الشافعي وغير شارح المقامات الحريرية (المرجع: المسعودي، مروج الذهب ومعادن الجوهر، المكتبة العصرية بيروت، ط/1، ج/1، 2005، ص 05) .

3 – المصدر نفسه، ص: 15 .

4 - Germy Philips, Alisen Fifth .Introduction to intellectual property low .1990.P:03

5 – عبد الرزاق السنهوري، شرح القانون المدني، ج8، ط3، 1964، ص: 206.

6 – ينظر: أحمد فضل شبلول، حول واقع الملكية الفكرية وحقوق المؤلف على شبكة الانترنت مقال الكتروني على صفحة الواب بتاريخ: 08 – 07 – 2015 .

7 – يوسف مكرم، تاريخ الفلسفة الحديثة، الناشر: مكتبة الدراسات الفلسفية، دار المعارف، ط/5 القاهرة، ص:151 .

8 – عامر محمد الكسواني، الملكية الفكرية ماهيتها، مفرداتها، وطرق حمايتها، دار الجيب للنشر والتوزيع،عمان،1998، ص: 72 .

9 – وداد أحمد العيدوني، حماية الملكية الفكرية في البيئة الرقمية: برامج الحاسوب وقواعد البيانات أنموذجا، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات، الرياض، 2010، ص: 04 .

10 – ينظر: بكر بن عبد الله أبو زيد، فقه النوازل، مؤسسة الرسالة، ط/1، 1996، ص: 158.

11 – أحمد محمد الصالح، الانترنت والمعلومات بين الأغنياء والفقراء، مركز البحوث العربية دار الأمين للنشر والتوزيع، القاهرة، ط/1، 2001، ص: 53 .

12 – أحمد محمد الصالح، الانترنت والمعلومات بين الأغنياء والفقراء، ص: 53 .

13 – ينظر: شريف درويش اللبان، تكنولوجيا النشر الصحفي، الدار المصرية اللبنانية، ط/1 القاهرة، 2001، ص:155.

14 – محمد فتحي عبد الهادي، تكنولوجيا المعلومات في المكتبات ومراكز توثيق المعلومات العربية بين الواقع والمستقبل، مكتبة الدار العربية للكتاب، القاهرة، 2000، ص: 288.

15 – أحمد محمد الصالح، الانترنت والمعلومات بين الأغنياء والفقراء، مركز البحوث العربية دار الأمين للنشر والتوزيع، ط1/، 2001، ص: 58 .

16- ينظر: أحمد محمد الإمام، الملكية الفكرية لقواعد البيانات في القانون السوري والمقارن مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثاني، 2013، ص: 338 .

السرقات الإلكترونية: تجلياتها وانعكاساتها على البحث العلمي، وسبل الحد من مخاطرها.

الدكتور حاجي الصديق
جامعة الإخوة منتوري، قسنطينة.

مقدمة: في عالم يزداد انفتاحا وتواصلا، وفي عصر يشهد ثورة علمية وتكنولوجية عارمة، وانتشارا واسعا لوسائل الإعلام والاتصال، التي تمثل الشبكة العنكبوتية قمة إبداعاتها، والتي ما لبث الواقع المعرفي يأخذ نصيبا من غاياتها ورهاناتها، ويستفيد من خدماتها وتطوراتها، والتي استطاعت تغيير الكثير من مظاهر الحياة، والأعمال والسلوكيات، خاصة فيما يتعلق باستخدام شبكة الأنترنيت التي أضحت تشكل الوعاء الأكبر للمعارف في هذا العصر، حيث غمرت العالم بدفق معلوماتي غزير يصعب السيطرة عليه.

ومن هنا أضحت مسألة السلامة المعلوماتية، تعكس تمثلا جديدا آخر للأنترنيت كمصدر للمخاطر المتعددة بشتى أنواعها، بداية من الإرهاب وصولا إلى مفاهيم مثل تهديد سلامة المعلومات والمبادلات التجارية وغيرها، ولعل أخطرها ظاهرة السرقات الإلكترونية.

لقد سمعنا عن بحوث ورسائل وأطروحات علمية كثيرة من ماجستير ودكتوراه تُسرق أو تُترجم بالكامل من شبكة الأنترنيت، والتي أخذت وضعا خطيرا وحرجاً ومؤلماً للغاية بجامعاتنا. وهو ما يؤكده الباحث الخبير الدكتور بلعيد صالح بقوله: "إننا ــ نحن المشرفين ــ تأتينا أبحاث الماجستير، الماستر، الدكتوراه، مقالات للتقويم...بعضها منسوخة نسخا كاملا، إلا في المقدمات والخواتيم، وبعضها مسروقة في أجزائها دون إشارة، وبعضها فيها القليل من التصرف، بعضها من

ترجمة واعتبارها من الإبداع، بعضها تصنف في العمل العلني couper-coller بعضها يغيب فيها مواصفات الباحث الناجح، واحترام عمل السابق...

وهذه الأشياء أبانته بعض الأبحاث التي وقع تجميدها بسبب فعل من الأفعال المخلة بأخلاق الباحث، بسبب الغش والسطو وما يتبعهما. كل هذا يحصل، ودون وازع ضمير، ... حالات كثيرة ليس من السهل السيطرة عليها، لأنها بدأت من حرم الجامعات" [(1)].

أُمورٌ يضحك السُّـــفهاء منها *** ويَـــبكي من عواقبها الحليم

إنّ وجود ذلك الكم الهائل من المعلومات على شبكة الأنترنيت، وسهولة الحصول عليها، يجعل من السهل القيام بعمليات القرصنة، والسطو على المواد المنشورة، من خلال إنزال هذه المواد أو نسخها، دون التحقيق من صدقها، ودون إخضاعها للمصدر، ونظرا لصعوبة متابعة ومراقبة كل ما ينشر على الشبكة بجميع لغاتها، فإنه يصعب اكتشاف السرقة بسهولة. فكانت بذلك أشبه بتجارة تتستَّر بالظلام، شـــأنُها التحايل في الارتزاق، لِـــتُـفسِدَ أسواق العلوم :

قد تَـــجِــــرَت في سوقنا عقربٌ *** لا مرحباً بالعقرب الـــتَّاجرة

إن مِن أسباب حِــفْــظِ العلم أن يسير وفق منهج علمي صحيح له خطة مرسومة، وغاية منشودة، لا يورث الباحث شعوراً بعبث موقفه، بحيث تتقطَّع أمامه سبل الطلب، فتسرق منه أبحاثه وتُنسب لغيره، ولا يجد من ينتصر له ويُنصفه في مظلمته، فلا يرى معنىً لقول الشاعر:

يا من يحاول بالأماني رتبتي *** كم بين منخفضٍ وآخر راقي

أأبيتُ ليلي ساهراً وتُضيعُهُ *** نوماً، وتأمل بعد ذاك لحاقي

لقد كان النقل المقترن بالعَــزْوِ والإحالة على المصدر ضابطا لا يتعدّاه كل من ينتسب إلى مجال البحث والإنتاج والمعرفة، وهو أمر دَرَجَ عليه الباحثون قديما من غير نكيرٍ من أحد، حتى صار عُرفا بين الباحثين، أما النقل عن الكتب من غير

إحالة عليها، فلا يتوجَّه إليه الضمير الحي بحال. وهو معنىً لم يَـــغِـــب عن الناس حتى في الجاهلية، فقد قال قائلهم:

ولا أغير على الأشعار أسرقها *** منها غَـــنِـــيتُ وشـــرٌّ الناس من سرقا

إن في التاريخ منبهة إلى أجلى مظاهر الرُّقِـــيّ في الأمم، وهو حسن الخلق وقوَّة التعليم وجودة التأليف فيه، فهما معياران دقيقان بهما يُـــقاس تـــقـــدُّم الأمم ورُقـــيُّها، وهما أمران يَفرضان على المجتمع عُقولاً حية مستنيرة، تُغالب الجهل وظُلمته..

وعليه، فإن الأمر يستحق بذل الكثير الجهد، من أجل ضرورة التقيد بحسن استخدام هذه التقنية العصرية بصرامة ووعي ومسؤولية جادة، ووفق الأطر القانونية والأخلاقية الضابطة لهذه العملية، من أجل مكافحتها ومحاصرتها، ومن ثمة السيطرة عليها.

وهي الحقيقة التي تدفعنا إلى التساؤل بحثا عن إجابات تثير المزيد من الأسئلة حول أبعاد هذه الظاهرة، وانعكاساتها على البحث العلمي، وفشوها بين أوساط الأدباء والكتاب والباحثين، ومخاطرها على الملكية الفكرية، والأمن المعلوماتي الذي يعد مجالاً خصبا واسعاً ذا أوجه عدة.

ولذلك فقد رأينا أنه من المهم أن نركّز جهودنا على مجالات الأمن المعلوماتي التي تخص مجال البحث العلمي، هذا المجال الذي ظهرت سلبياته أيضا بشكل جلي، لا يمكن لأحد إنكارها، حيث تجلت في نوع جديد من الإجرام المعاصر ارتبط وتطور بتطور الحياة، والأنشطة الاقتصادية والوسائل التكنولوجية، لا سيما في ظل انتهاج الدول لسياسة العولمة؛ والتي دعمت عناصرها وتقنياتها بشكل كبير هذا النوع من الإجرام، ولم تجعل منه إجراما وطنيا يقتصر في نطاق الإقليمي للدولة فقط، وإنما أصبح يكتسب طابعا عالميا متزايدا، مما خلق تحديا جديدا تواجهه السياسات الجنائية، وهو الجريمة المنظمة بكافة أشكالها ؟

من هنا كان لزاماً علينا أن ينفر في كل قطر من بلادنا من ينهض بشأن الأخلاق والتعليم، ويجب على الجامعات في بلادنا أن تهتم بذلك، وأن تتميَّز بجودة الأبحاث والسَّبق فيها، وأن تبني طلاَّبها، وتحصِّنهم بحسن الخلق، والعلم والرحلة في طلبه حتى يَرتاضوا الأبحاث الجادة والمبتكرة.

واستنادا إلى ما تقدم، بات من المُلح أن نقف عند هذه الظاهرة، لتمحيصها ودراستها، وتحديد أبعادها وأسبابها وانعكاساتها السلبية على الفرد والمجتمع، وذلك لمعرفة الخلاصة التي يمكن أن نصل إليها لتوصيف مآلات هذه الطفرات الإعلامية والتكنولوجية التي لا تتوقف. هل ستجعل حياتنا تتجه إلى ما هو أفضل؟ أم أنها ستؤول بنا إلى ما هو أسوأ؟

وتبقى الغاية والمنطلق من كل ذلك، هو تحديد إطار خطة عمل جاد، يمكن من خلاله التأسيس لثقافة قانونية ردعية، وغرس قيم اجتماعية وتربوية وأخلاقية بهذا الشأن، حتى نتمكن من تطوير هذه الثقافة إلى سلوك حضاري نمارسه بقوة الفعل والعمل.

ومن هذا المنطلق يستمد هذا الموضوع أهميته ومشروعيته بالنظر إلى دور البحث العلمي، ومكانة الجامعة التي تعتبر في العرف العالمي ركنا أساسيا في الحياة الثقافية والعلمية والمعرفية، وفي أيّ بلد من بلدان المعمورة، وأكثر من ذلك فهي بمثابة العقل المفكر والمدبر، الذي بدونه لا يمكن أن تتحقق التنمية بكل أنماطها،_لا سيما في ظل العولمة، ومجتمع المعرفة وثورة المعلومات، وما أحدثته هذه الأخيرة من تأثير في مختلف مناحي النشاط الانساني.

وفي ظلّ هذه المؤشرات تحاول هذه الورقة أن تقدم صورة عن هذه الظاهرة مع الإشارة إلى الجهود المبذولة من قبل وزارة التعليم العالي والبحث العلمي في الجزائر بإدراج «السرقات العلمية» ضمن بنود أخلاقيات الجامعة، والتي تصنفها في خانة الأخطاء الجسيمة، التي تؤدي بصاحبها إلى الطرد والمتابعة القضائية

ومع ذلك فالسرقات متواصلة، وهي الحقيقة التي تتجلى أكثر فيما تستقبله الوزارة سنوياً من العديد من الشكاوى والمراسلات المتعلّقة بسرقات علمية مختلفة.

فما الذي ساهم في انتشار هذه الظاهرة؟ وما هي آثارها؟ وما هو واجبنا نحوها؟ ولماذا لا يخجل الطالب أو الأستاذ من سرقة جهد غيره، ثم ينسبه لنفسه بكل بساطة، وبدون أدنى حرج؟ وفي هذه الحال أيُّ تَقدُّم يُرتجى؟ وأيُّ نُهوض يُـــرتقب؟ وعليه ما هي الحلول التي يمكن أن تحدّ من ظاهرة هذه اللصوصية التي أصبحت تطال البحوث والدراسات العلمية الجامعية؟

وقبل أن نجيب عن هذه التساؤلات، ومما له علاقة بهذه الظاهرة المشينة بجامعاتنا، يحسن بنا منهجيا أن نقف أولا عند مصطلح السرقة العلمية. فما المقصود بهذا المصطلح ؟

1 ــ مفهوم السرقة: إن المتتبع لهذه الكلمة في المعاجم اللغوية [(2)] . يجد أنها تدل على أخذ الشيء من الغير خفية، لغاية نفعية. فالملكية ركن أول، والاعتداء ركن ثان، وبدونهما لا يجوز الادعاء بوجود السرقة. وهي من حيث طبيعة المسروق نوعان: حسي ومعنوي. والأول يتعلق بملموس قابل للانتزاع أو الإخراج أو النقل من حيازة صاحبه وبدون رضاه.

أما الثاني فينطبق على عالم الفكر والعاطفة والخيال.

وعليه فالسرقة العلمية في مفهومها الاصطلاحي: تعني استخدام أفكار الآخرين أو مناهجهم، أو أبحاثهم، أو ألفاظهم أو عرضها دون اشتشهاد لائق. وهو ما يحدث حين يهمل الباحث توثيق هذه الأعمال والأفكار الأصلية، مما ينجم عنه أن يفهم القارئ أنّ ما ذكر في بحثه هو من بنات أفكاره هو نفسه، وليس نتيجة دراسة شخص آخر.

وتحدث السرقة العلمية سواء أعاد الباحث صياغة ما كتبه، أو ذكره شخص آخر، أو استخدم ألفاظه حرفيا دون ذكر للمرجع المستخدم. وتعتبر نتائج السرقة

العلمية واحدة في جميع الأحوال بغض النظر عن نية الباحث محل المساءلة، وهي جريمة تستحق عقابا حازما.

وقد تنوعت في هذا السرقة بتنوع المناحي الكتابية العلمية والأدبية، كسرقة الشعر وسرقة الأفكار والأقوال، وسرقة المصنفات، حيث لم تقتصر السرقة العلمية على المقالات والأبحاث المختصرة، بل امتدت إلى الرسائل الجامعية، والبحوث بأكملها، وتباينت في ذلك أشكالها وألوانها ومصطلحاتها، فمنها ما عرف بالسلخ: وهو أخذ بعض المعنى، ومنها ما عرف بالمسخ : وهو إحالة المعنى إلى ما دونه ومنها ما عرف بالنسخ: وهو أخذ المعنى واللفظ جميعا.

ولا غرابة أيضا أن عرفت لها مرادفات تنطوي على بعض المفارقات كالخلس: وهو اختطاف الشيء بسرعة وعلى غفلة، والطر: وهو الشق والقطع والنهب، والخرابة : وهي سرقة الإبل خاصة، ثم استعيرت لكل من سرق بعيرا أو غيره [3].

ومهما يكن من أمر، وأيا كان المأخذ والآخذ والمأخوذ، فإن السرقة تعد من الآفات القديمة والحديثة، وهي التي تعرف اليوم بالسطو أو القرصنة الفكرية "أو الاعتداء على حق الغير، ولذا فمحاربتها لزومية، لأنها تطرف، والعمل على كشف أصحابها من أوجب الواجبات، فهي بمثابة الخيانة في العار والخسة والسخف والدناءة وجلب المسخطة من المعتدى على ملكه، ولهذا فقد شنع القدماء والمحدثون بأصحابها [4]، وما ذلك إلا من صدق الإيمان، فالمؤمن لا يطبع على الخيانة والبهتان. يقول ابن المقفع في النهي عن انتحال رأي الغير: "إن سمعت من صاحبك كلاما، أو رأيت منه رأيا يعجبك، فلا تنتحله تزينا به عند الناس، واكتف من التزين بأن تجتني الصواب إذا سمعته، وتنسبه إلى صاحبه. واعلم أن انتحالك ذلك مسخطة لصاحبك، وأن فيه مع ذلك عارا وسخفا. فإن بلغ بك ذلك أن تشير

برأي الرجل، وتتكلم بكلامه، وهو يسمع جمعت مع الظلم قلة الحياء، وهذا من سوء الأدب الفاشي في الناس"[5].

وفي ذات السياق يقول السيوطي في مقامته "الفارق بين المنصف والسارق" كاشفا عن خيانة من تجرأ على سرقة بعض كتبه[6]: "هل أتاك حديث الطارق؟ وما أدراك ما الطارق؟ الخائن السارق، والمائن المارق... فما كان من هذا العديم الذوق إلا أنه نبذ الأمانة وراء ظهره وخان، وجنى ثمار غروسنا، وهو فيما جناه جان، ... وعمد إلى كتابي "المعجزات والخصائص" المطول والمختصر، فسرق جميع ما فيها بعباراتي التي يعرفها أولو البصر، وزاد على السرقة، فنسبهما إلى نفسه ظلما وعدوانا وما اقتصر، وقال: تتبعت وجمعت ووقع لي".

ونقل النصوص من الكتب دون عزوها لأصحابها، لطخ بتهمة الخيانة من لبس الزور في انتحال ما ليس له، وهذا في شتى العصور، لأن الأمانة من الإيمان والخيانة من المكر والخديعة، وكلهن في النار. وذلك لكونهن من الدنايا التي تقتل يقظة الضمير، وتستحل اقتطاع حقوق الغير.

ولا نجد هذا عند أشرف الناس طباعا، وأقواهم إيمانا، وأزكاهم معدنا، وإنما عند المهازيل المنافقين المتنكرين للحق، والمهملين للواجب والأمانة العلمية، ومن ثمة حظيت السرقات العلمية بالحديث والتخريج والتجريح، دفاعا عن أداء الأمانة وتشنيعا بخساسة سخف الخيانة.

وانطلاقا من هذه الحقيقة الصارمة، بات من اللافت للانتباه، في ظل هذه المعطيات، وما نعيشه من تحديات في ظل مجتمع المعلومات، وتسارع وتيرة التغيرات عبر العالم، ومنجزات التقدم التقني معالجة هذه المعضلة، الظاهرة الخطيرة، التي تتنزل في صميم وعمق القضايا والإشكاليات العلمية والأخلاقية والتربوية المعاصرة، التي باتت تطرحها شبكة الأنترنيت، نتيجة سوء استخدامها والتي أضحت أحيانا محرضًا خطيرًا على كثير من الانتهاكات لأسباب نفسية

شخصية، أو قناعات إيديولوجية جماعية، فكان الوعي المعلوماتي أهم مقومات الأمن المعلوماتي [7].

وذلك من خلال تقديم الرؤى، والوسائل الفاعلة، وسن القوانين لتجريم السطو على الملكية الفكرية، واتباع خطة عمل يمكن من خلالها التأسيس لثقافة قانونية ردعية، وغرس قيم اجتماعية وتربوية وأخلاقية أصيلة بهذا الشأن.

وهي الحقيقة التي تدفعنا إلى التساؤل بحثا عن إجابات تثير المزيد من الأسئلة حول أبعاد هذه الظاهرة وانعكاساتها على البحث العلمي، وفشوها بين أوساط الأدباء والكتاب والباحثين، ومخاطرها على الملكية الفكرية، والأمن المعلوماتي الذي يعد مجالاً خصبا واسعاً ذا أوجه عدة، ولذلك فقد رأينا أنه من المهم أن نركّز جهودنا على مجالات الأمن المعلوماتي التي تخص مجال البحث العلمي، هذا المجال الذي ظهرت سلبياته أيضا واضحة بشكل جلي، لا يمكن لأحد إنكارها حيث تجلت في نوع جديد من الإجرام المعاصر ارتبط وتطور بتطور الحياة والأنشطة الاقتصادية والوسائل التكنولوجية، لا سيما في ظل انتهاج الدول لسياسة العولمة؛ والتي دعمت عناصرها وتقنياتها بشكل كبير هذا النوع من الإجرام، الذي سوف يقودنا حتما إلى فوضى علمية وأخلاقية، ويقطع سبل التطور والحضارة ويجب أن نعلم أن هذا الإجرام، لم يعد إجراما وطنيا يقتصر في نطاق الإقليمي للدولة فقط، وإنما أصبح يكتسب طابعا عالميا متزايدا، مما خلق تحديا جديدا تواجهه السياسات الجنائية، وهو الجريمة المنظمة بكافة أشكالها. ؟

وعليه، فإن الأمر يستحق منا بذل الكثير الجهد من أجل ضرورة التقيد بحسن استخدام شبكة الانترنت، واستثمار هذه التقنية العصرية بصرامة ووعي ومسؤولية جادة، ووفق الأطر القانونية والأخلاقية الضابطة لهذه العملية، من أجل مكافحتها ومحاصرتها، ومن ثمة السيطرة عليها، لاسيما إذا علمنا أننا من الدول الأضعف في التصنيف العالمي من حيث الأمن المعلوماتي.

أسباب السرقة العلمية:

إن السرقات العلمية في الجامعة هي في الواقع نتيجة منظومة مُتعدّدة الخلفيات والحلقات، فلئن كان الطالب أو الأستاذ هو الحلقة الأخيرة التي تعلق بها تهمة السرقة العلمية –إن تم اكتشافها– فإن وراء هذه الضحية الأخيرة منظومة مُتعدّدة الحلقات، فقدَ فيها الباحثُ أصول التكوين العلمي، وأخلاقيات البحث، والرقابة البيداغوجية، والتأطير السليم، وخلف كل ذلك سياسة تعليمية صارمة تفرض قانونها على الجميع. وعليه فأسباب السرقة العلمية مُتعدّدة تبدأ من المدرسة، ربما يعود السبب الأول إلى ضعف المنظومة التربوية التي تدفع بآلاف المتعلمين إلى الجامعات دونما كفاءة، ليجدوا أنفسهم أمام معارف تفوق طاقاتهم، فيحتالون عليها بالتواطؤ مع مؤسساتهم ومكونيهم، فينجحون دون استحقاق، ويضطرون إلى إعداد بحوث لا يمتلكون غالباً ما يؤهلهم علمياً لإنجازها فيلجؤون إلى الحل السهل، وقد وفرت التكنولوجيا العلمية هذا الحل.

والسبب الآخر يتعلّق بالأساتذة، فهم لم يتحملوا مسؤوليتهم ووقعوا ضحية هذا السقوط العام، فتخلّوا، كما تخلّى الجميع، مؤسسات وأفراداً، عن مفهوم العلم بوصفه رسالة، إلى مفهومه بوصفه شهادة. تساهل الكل واتفق الجميع على الجريمة.

والسبب الثالث يعود إلى المؤسسات الإدارية والعلمية التي انخرطت في الرداءة وانضمت إلى جحافل المتآمرين ضد العلم.

والسبب الرابع، ما نراه من انسداد الأفاق أمام الطلاب، فليس ثمة دافع قوي يدفعهم إلى العلم وهم يرون من سبقهم من أصحاب الشهادات تلقي بهم الجامعات إلى المجهول.

ومن أجل معالجة الأمر لا يكفي الوقوف عند الأسباب الأربعة المذكورة، بل ينبغي الذهاب إلى استعادة القيمة الغائبة قيمة العلم وإلى إعادة الاعتبار للمعرفة ليست الجامعة هي المتضررة من فكرة سقوط القيم العلمية، بل المجتمع كله حاضراً ومستقبلاً، وإذا استمر هذا السقوط فسيكون من الصعب مستقبلاً إيجاد أي حل، لأننا لن نكون عندها أمام الحالة المرضية فقط، بل أمام مضاعفاتها.

وعلى الرغم من الجهود المبذولة، بإدراج وزارة التعليم العالي والبحث العلمي في الجزائر «السرقات العلمية» ضمن بنود أخلاقيات الجامعة، والتي تصنفها في خانة الأخطاء الجسيمة، أي من الدرجة الرابعة التي تؤدي بصاحبها إلى الطرد من المؤسسة الجامعية والمتابعة القضائية .

ومع ذلك فالسرقات متواصلة، وهي الحقيقة التي تتجلى أكثر فيما تستقبله الوزارة سنوياً من العديد من الشكاوى والمراسلات المتعلّقة بسرقات علمية مختلفة.

نعم لقد حان الوقت لتقديم الإجراءات والآليات الضرورية لمواجهة ظاهرة "السرقة العلمية"، كونها تمس بمصداقية الجامعة الجزائرية، وهو ما يقتضي معاقبة كل من يقوم بها، وذلك من أجل الحفاظ على الأمانة العلمية والأخلاقيات الجامعية.

فالأمانة العلمية أخلاق وقيم، ينبغي أن تتنزّل في صلب البحث العلمي، وفي إنجاز البحوث والمذكرات والرسائل الجامعية، بل هي من أخلاق المثقفين والباحثين، وأنّ من يسرق أفكار الآخرين، وينسبها لنفسه كمن أرتكب جُرماً كبيراً بل قد تكون تهمته أعظم ممن يسرق الأموال والأشياء ذات الطابع المادي. وقد نشأ جيل بكامله على هذه التوجيهات والنصائح، بل عِدّة أجيال. كان آنذاك الغش استثناء والالتزام بالأخلاق والقوانين هو القاعدة، وفي هذا الإطار تم إصدار تعليمة من وزارة التعليم العالي والبحث العلمي تحمل رقم 1217/أ خ و/2013 بتاريخ 19 ديسمبر 2013 جاء فيها أنه "بسبب كثرة المراسلات التي تنبه إلى حالات السرقة العلمية في النشريات، والمقالات العلمية، وأطروحات الدكتوراه، تحتم علينا ضرورة معالجة هذه المسألة بطريقة ناجعة، قبل أن تأخذ هذه الظاهرة أبعادا يصعب تداركها، وعليه ينبغي التفكير في وضع قواعد وأنماط تحكم الأمانة العلمية وتنشط آليات المتابعة وتطور المنتوج العلمي للأساتذة الباحثينن والباحثين الدائمين الجزائريين، وفق شروط الأخلاقيات الجامعية وآدابها الأكثر صحة والأكثر قبولا".

وتواصل التعليمة بأن "مسؤولية الأسرة العلمية، وعلى الخصوص الأساتذة الباحثون والباحثون الدائمون، كبيرة في الحد من هذا السلوك، فدور الهيئات

الإدارية يأتي عند المعالجة البعدية لهذه الحالات، ومن البديهي أن مدير الأطروحة والمشرف على أعمال البحث، هو في الغالب الفاعل الأول المكلف بمتابعة كل مراحل البحث، لذلك فهو الضامن لأصالة وأمانة العمل العلمي"، كما أن "الخبراء وأعضاء اللجان المكلفين بتقويم عمل البحث ومناقشته، هم أيضا مسؤولون عن نوعية هذا العمل، ويمكن للمجالس العلمية للمؤسسات على مستواها أن تساهم إيجابيا وبطريقة بناءة في هذه العملية". وعليه كان "من المستعجل وضع قواعد وأنماط لتأطير صيرورة عمل البحث واتخاذ إجراءات ملموسة ومحكمة مشتركة بين كل المؤسسات الجامعية والبحثية، لضمان أمانة وأصالة كل منتوج علمي وجعل أولوية نخبة باحثينا في الاهتمام بالجوهر، وهو تنظيم مساهمة أسرتنا العلمية في إنتاج المعرفة وتطوير المعرفة العالمية".

إن هذا الموضوع الحساس يقتضي اتخاذ كافة الإجراءات على مستوى المؤسسات الجامعية للقضاء على هذه الظاهرة، من خلال تكريس إجراءات وقائية وأخرى ردعية. باعتبار أنّ هذه المسألة أصبحت تُخلّ بنزاهة الطلبة والأساتذة كما تخل بسمعة الجامعة، والمنتسبين إليها، وبقيمة البحث العلمي، الذي أصبح في حالات معينة فاقداً في معظمه للنزاهة والمصداقية والمهنية العلمية. فالسرقات المتكرّرة للبحوث العلميّة تدل على أن الظاهرة تستفحل يوماً بعد آخر في جسد الجامعة، وفي حرمها الذي أنهكته وانتهكته لصوصيّة من نوعٍ آخر، لصوصيّة لم تحترم الأمانة العلمية وتطاولت على مجهود الآخرين بغير حق.

والحل في نظري هو الصرامة في معاقبة كل من يقوم بأفعال السرقة العلمية وفضحهم، وعدم التستر عليهم، وذلك وفقا للتنظيم الساري المعمول به، بما في ذلك اللجوء إلى العدالة، كما تعد مشاركة اللجان المحلية لأخلاقيات المهنة الجامعية وآدابها في هذه المسألة أساسي، وعليه فإنه من الضروري تنشيط أعمالها، للتكفل بمعالجة حالات السرقة العلمية التي تعرض عليها.

ومن الإجراءات الوقائية التي تم تبنيها منها إجبار أصحاب الأبحاث العلمية على إيداعها قبل وبعد مناقشة أطروحاتهم، علاوة على فتح موقع إلكتروني عبر شبكة الأنترنت من أجل التعريف بالأبحاث العلمية ونشرها على نطاق أوسع بغرض ضمان مقروئية أكبر لها، وهو ما من شأنه الحد من سرقتها.

والجدير بالذكر في هذا الإطار أنه "تم – وعلى المستوى العالمي – تطوير برنامج للإعلام الآلي بإمكانه رصد السرقات التي تطال الأبحاث العلمية غير أنه يبقى محصورا في الأعمال المكتوبة باللاتينية دون العربية."[8]

وهنا يحسن بنا أن نتساءل: هل عدم توفر هذا الجهاز حاليا فتح المجال للبعض في غفلة من أمرهم إلى حمل شعار: "اسرق قليلا من بحوث وجهود الآخرين تصبح دكتورا".

هل حقيقة تنام بعض الجامعات الجزائرية من خلال العديد من المعاهد والكليات على فضائح لا حصر لها لسرقات علمية المتورط فيها أساتذة جامعيون ومسؤولون جعلت منهم دكاترة وباحثين بشهادات كارتونية لا تحمل غير الاسم، لتشرع وزارة التعليم العالي في جملة من التحقيقات التي أحيل أغلبُها على المحاكم؟[9]

وتذكر بعض المصادر على الشابكة أنّ فضائح السرقات العلمية طالت سمعة الجامعة الجزائرية في الخارج، بسبب سرقة العديد من المذكرات من بلدان عربية وأوربية وإعادة طبعها في الجزائر على أنها "بحوث علمية جديدة".

وبالرغم من ذلك يبدو أن السرقات العلمية تحولت إلى آفة متجذرة في سلوكات بعض المتعلمين، ولعل مكمن الخطر أنها امتدّت أيضا إلى تلاميذ المدارس الذين باتوا ينسخون البحوث الجاهزة من مقاهي الأنترنيت، وهذا ما ساهم في تجميد عقول التلاميذ الذين يألفون ظاهرة سرقة البحوث الجاهزة. فماهي الحلول؟ وما هي الاقتراحات؟

الاقتراحات والحلول:

1 ــ العمل على إعداد إستراتيجية وطنية شاملة للتعامل مع قوانين عصر المعلومات، وذلك من خلال الاهتمام بدراسة الجوانب المتعلقة بالأمن المعلوماتي على الصعيدين القانوني والتقني، ومن ثم الحد من ظاهرة السرقات العلمية بالحديث عنها وكشفها والتبليغ عنها والمطالبة بمحاربتها.

2 ــ ضرورة تفعيل القوانين المرتبطة بالمعلوماتية ميدانيا، حتى لا تبقى حبرا على ورق، وتكثيف الجهود العلمية وعقد الندوات لإعطاء هذه القوانين ما يجب من عناية.

3 ــ إحداث شرطة قضائية متخصصة في مجال مكافحة الجرائم المعلوماتية تجمع ما بين التكوين القانوني والتكوين التقني، مع اعتماد أسلوب الفريق المعتمد في إدارة المشروعات، الذي تقوم فلسفته على الاستخدام الفعال لمجموعة متنوعة من المتخصصين في مهمة واحدة.

4 ــ وضع مشروع قانون يتلاءم وطبيعة خصائص الجريمة المعلوماتية، وفق ما يحمله من مقتضيات إجرائية تراعي خصوصية الجرائم المعلوماتية، مع اقتراح إحداث سلطة وطنية مستقلة يكون من بين اختصاصاتها فحص النظم المعلوماتية على المستوى الوطني، فضلا عن وجوب التكامل في الجهود العربية نحو المعلوماتية والتكنولوجيا، وربط ذلك بقضايا الأمن القومي والتنمية.

5 ــ التركيز على الجوانب التقنية في المجال المعلوماتي، والمتعلقة بالخصوص بالتوقيع الالكتروني، وعمليات التشفير والآليات القانونية لتكريس الأمن المعلوماتي، وحماية المعطيات القانونية والسر المهني والنشر الالكتروني والحقوق الرقمية الأساسية وبرامج الحاسوب.

6 ــ حصر الجرائم المعلوماتية من أجل تحديد طبيعتها القانونية، وإبراز خصوصيتها والإشكالات المرتبطة بها، وضبط مواصفات الشرطة القضائية المتخصصة فيها، والعمل على تفعيل قواعد القانون الجنائي في تحقيق الحماية

منها، وكذا السياسة الجنائية المتبعة فيها، والانخراط في مسلسل التعاون الأمني الدولي في هذا المجال، وذلك بغية توسيع آفاق التعاون في مجال مكافحتها.

الهوامش:

---

1 ــ اللغة الجامعة، صالح بلعيد، منشورات مخبر الممارسات اللغوية في الجزائر، جامعة مولود معمري، تيزي وزو، 2015 ص: 170.

2 ــ ينظر المعجم العربي الأساسي، لاروس، المنظمة العربية للتربية والثقافة والعلوم، تأليف جماعة من كبار اللغويين العرب، 1989، مادة سرق، ص: 620.

3 ــ ينظر: لسان العرب، لابن منظور، مادة: سرق. والمعجم العربي الأساسي، لاروس، المنظمة العربية للتربية والثقافة والعلوم، تأليف جماعة من كبار اللغويين العرب، 1989، مادة سرق ص: 620.

4 ــ ينظر: السرقات العلمية، دراسة وتقسيما وعلاجا، لحسان عبد المنان، دار ابن حزم للطباعة والنشر، ط1، 1996، ص: 4 وما بعدها. والأدب الصغير والأدب الكبير، لابن المقفع، دار صادر بيروت، ص: 98. ومقامات السيوطي، شرح وتحقيق: سمير الدروبي، مقامة ــ الفارق بين المنصف والسارق.

5 ــ الأدب الصغير والأدب الكبير، لابن المقفع، دار صادر بيروت، ص: 98.

6 ــ مقامات السيوطي، شرح وتحقيق د| سمير الدروبي، مقامة "الفارق بين المنصف والسارق".

7 ــ اللغة الجامعة، صالح بلعيد، منشورات مخبر الممارسات اللغوية في الجزائر، جامعة مولود معمري، تيزي وزو، 2015 ص: 162.

8 ــ منتدى الهامل، عالم الأخبار الدولية: اسرق قليلا من بحوث الآخرين تصبح دكتورا.

9 ــ (الجريدة الرسمية العدد رقم 23 المؤرخ في 4 ماي 2008)، فإن السرقات العلمية، تعد من الأخطاء الجسيمة غير المبررة التي يمكن أن تؤدي إلى الطرد".

الرسائل العلمية الجامعية في المكتبات الرقمية بين النفاذ الحر للمعلومات وسرقات الملكية الفكرية

أ. نزهة خلفاوي وأ. سعاد عباسي
مركز البحث العلمي والتقني لتطوير اللغة العربية
وحدة البحث، تلمسان

تمهيد: إن الثورة العلمية والتكنولوجية التي يشهدها العصر تجعلنا نتجه نحو الحكومة الإلكترونية في جميع المجالات، فقد أصبح النظام الرقمي شيئا فشيئا يحكم جميع تعاملاتنا حتى العلمية منها، فالتطور في تكنولوجيا المعلومات والاتصال فرض علينا تغيير أنظمة حفظ واسترجاع الرسائل الجامعية، حيث اتجهت الجامعة الجزائرية في ظل هذا التطور إلى إنشاء المكتبات الإلكترونية التي تضمن مجانية وآنية تلقي البحوث العلمية الأكاديمية طلبا لتثمينها وتطوير البحث العلمي.

هذا ما يجعلنا نقف عند إشكالية حقوق الملكية الفكرية للمنشورات الجامعية الرقمية والدفاع عن المجهودات والمكتسبات العلمية من خلال طرح التساؤلات الآتية:

– هل تستطيع المكتبات الرقمية الجامعية تحقيق مساعيها لإتاحة النفاذ الحر للمعلومات مع ضمان تجاوب إيجابي من قبل مستخدميها؟

– كيف تستطيع المكتبات الجامعية الرقمية تثمين البحث العلمي وتطويره مع الحفاظ على الملكية الفكرية لأصحاب الرسائل العلمية المنشورة على مواقعها؟

ما هي استراتيجيات التصدي للسرقات العلمية الإلكترونية بعد إطلاق مشاريع المكتبات الرقمية؟

بالإجابة عن هذه التساؤلات نتطلع للوصول إلى اقتراح استراتيجية لتفادي الوقوع في فجوة بين مساعي إنشاء وتفعيل المكتبات الرقمية الجامعية وواقع استخدامها.

أولا: النشر الإلكتروني للرسائل الجامعية: إن ما يشهده العصر من انفجار معلوماتي وابتكارات تكنولوجية جعل العالم يعيش تحولات عميقة مست كل الميادين، فمن الصناعة إلى السياسة إلى البحث العلمي أصبحت المؤسسات محاصرة بضغوطات كبيرة تحتم عليها مواكبة هذا التطور المتسارع.

والجامعة بصفتها إحدى مؤسسات البحث العلمي ليست بمنأى اليوم عن هذا الحراك التكنولوجي، فكل هياكلها مطالبة باللحاق بالركب ضمانا للجودة. ولعل المكتبة الجامعية من أهم الهياكل التي ترفع التحدي باحثة عن أنجع السبل للتكيف مع المعطيات الجديدة، ويعتبر النشر الإلكتروني من أهم التحديات المرفوعة اليوم على مستوى جامعاتنا .

1- مفهوم النشر الالكتروني: للوقوف عند مفهوم النشر الإلكتروني يتوجب علينا قبل ذلك التعريج على النشر المكتبي والذي يعرّفه أيمن السامرائي وعامر قنديلجي بأنه استخدام الحواسيب المايكروية في الطباعة. وكذلك هو نظام إنتاج طباعي قليل الكلفة، له القدرة على تركيب وتشكيل وتجميع كل من النص المكتوب والمخطوطات والأشكال المرسومة على شاشة عالية الجودة، مع برمجيات خاصة لهذا الغرض وضعت وصممت لجعل الطباعة عملية يمكن إتقانها والقيام بها من قبل أي شخص بعد تدريب بسيط. كما أنه عبارة عن برمجيات خاصة مع حواسيب مايكروية وطابعات ليزرية غير مكلفة تنتج صفحات منظمة ومعدة بصورة جذابة يمكن من خلالها الحصول على خطوط بأنواع وأشكال مختلفة ومتنوعة.[1]

أما شوقي سالم فيرى بأن النشر المكتبي هو تطبيق ناشئ للحواسيب المايكروية لتصميم وطباعة وثائق عالية الجودة بشكل كامل في المكتب ذاته دون إرسال أي

معلومات أو أعمال طباعية إلى الخارج، أو عند الانتهاء من إعداد الصورة الأصلية للوثائق فيمكن عندئذ إرسالها إلى شركة طباعية لإنتاج كميات منها.[2]

والنشر الإلكتروني هو أحد النتائج الهامة للعصر الرقمي وتقنياته الجديدة ويعتبر الركيزة الرئيسية للاتصال العلمي بين الباحثين، وهو نظام تخزين المعلومات[3] في مراصد المعلومات، ثم الاسترجاع والعرض منها لأي وثيقة أو جزء من وثيقة عند الحاجة بوسائط عرض أو بوسائل مطبوعة. والنشر الإلكتروني يشمل الكتب والوثائق والمجلات والدوريات الإلكترونية والرسائل الإخبارية، ونظم الاستفسار والإجابة ومواقع المعلومات على الإنترنيت.

وفي هذا السياق أورد حسن أبو خضرة تعريفاً للنشر يأتي في أحد ثلاثة أشكال:-

1. استخدام الحاسب الآلي لتسهيل إنتاج المواد التقليدية.
2. استخدام الحاسب الآلي ونظم الاتصالات لتوزيع المعلومات إلكترونياً عن بعد.
3. استخدام وسائط تخزين إلكترونية.

وهكذا فإن النشر الإلكتروني أسلوب جديد في النشر أفرزته التكنولوجيا الحديثة ويتمثل في إمكانية إنتاج ونشر وتوزيع المواد باستخدام وسيط إلكتروني سواء على أقراص مدمجة (مليزرة) أو عبر شبكات مثل شبكة الإنترنت كبديل للنشر المطبوع على الورق[4].

ويشير حسن أبو خضرة إلى أن بداية النشر الإلكتروني تعود إلى نهاية الستينات عندما بدأت بعض شركات النشر باستخدام الحاسوب في التنضيد الضوئي، وأظهر هذا الجيل الثانوي من الشريط الممغنط الذي أدى إلى إيجاد الدفعات والخدمات الآلية. وفي أواخر السبعينات قدمت أجهزة الحاسوب والاتصالات عن بعد فرصاً جديدة للنشر، أولها وأهمها أنها فتحت إمكان النشر الإلكتروني بناءً على الطلب كما

أصبح عملياً تخزين نسخة من عمل بدلا من الاستماع إليه أو مشاهدته وكانت تلك البداية الحقيقية للنشر بناءً على الطلب".[5]

والواقع يؤكد أن النشر الإلكتروني استفاد من تقنيات النشر المكتبي وتخطاه إلى آفاق أوسع، وبذلك لا يعد النشر الإلكتروني بديلا عن النشر الورقي؛ وعلى المدى البعيد فإن هذه المنشورات الإلكترونية سوف تقلل من الحاجة إلى استخدام المكتبة الورقية. ولعل من أبرز مزايا النشر الإلكتروني[6] ما يلي:

- **التفاعلية:** حيث يؤثر المشاركون في عملية النشر الإلكتروني عن طريق الاتصال بالآخرين وتبادل المعلومات معهم، مما يخلق التواصل والتفاعل. فمن خلال منصات النشر الإلكتروني سيظهر نوع جديد من منتديات الاتصال والحوار الثقافي المتكامل والمتفاعل عن بعد، مما سيجعل المتلقي متفاعلاً مع وسائل الاتصال تفاعلا إيجابياً.

- **اللاجماهيرية:** حيث يمكن توجيه النشر الإلكتروني إلى فرد أو مجموعة معينة من الأفراد.

- **اللاتزامنية:** حيث يمكن عن طريق النشر الإلكتروني القيام بالنشاط الاتصالي في الوقت المناسب للفرد دون ارتباط بالأفراد الآخرين أو الجماعات الأخرى.

- **الحركية:** وتعني إمكان نقل المعلومات عن طريق النشر الإلكتروني من مكان لآخر بكل يسر وسهولة.

- **القابلية للتحويل:** أي القدرة على نقل المعلومات عن طريق النشر الإلكتروني لها من وسيط لآخر.

- **الشيوع والانتشار:** بمعنى الانتشار حول العالم وداخل كل طبقة من طبقات المجتمع.

- **العالمية أو الكونية:** على أساس أن البيئة الأساسية الجديدة للنشر الإلكتروني ووسائل الاتصال والمعلومات أصبحت بيئةً عالمية.

- **القضاء على مركزية وسائل الإعلام والاتصال،** إذ ستعمل الأقمار الصناعية على القضاء على المركزية في نشر المعلومات والبيانات، ولن يرتبط الناس بوسائل الإعلام من خلال المسافات الجغرافية فقط، وإنما سيرتبطون معا من خلال اهتماماتهم المشتركة.

- **زوال الفروق التقليدية بين وسائل نشر المعلومات:** المتمثلة في الصحف والكتب والمجلات، حيث أصبح مضمون أي وسيلة منها عن طريق النشر الإلكتروني متاحاً ومشاعاً في جميع الوسائل الأخرى وبأشكال وأساليب عرض وتقديم مختلفة ومتطورة.

- **على المستوى العلمي والبحثي والجامعي** فإن النشر الإلكتروني يتيح الفرصة أمام الباحثين والجامعيين إلى توجيه الجزء الأكبر من جهودهم إلى عمليات التحليل والتفسير والاستنتاج والتنبؤ والكشف عن الظاهرات والمتغيرات الجديدة بدل ضياع نسبة كبيرة من جهد الباحثين في الحصول على المعلومات.

- **ضمان الجودة العالية للمخرجات المطبوعة:** وذلك نتيجة تطور البرمجيات والطابعات التي أصبحت تضاهي كفاءة منتجات المطابع المحترفة وجودتها، بشكل يصعب التفريق بينهما أحياناً.

- **ضمان الاقتصاد الملموس في الوقت والجهد والمال:** النشر الإلكتروني اختصر عمليات النسخ والطباعة والمتطلبات البشرية والمالية كلها وأصبحت الكلفة الحالية تقدر بعُشْر كلفة الطباعة التقليدية.

- **السرعة العالية في الإنجاز:** مع ضمان الجودة والكفاءة العالية وبأقل جهد.

يساهم النشر الإلكتروني في التغلب على العديد من المشاكل التي تنجم عن الكتاب المطبوع، كما أنه يساير التقدم العلمي في نشر المعارف، والحصول عليها بسرعة. وقد دخل بالفعل عدد ضخم من دور النشر الجامعية مجال النشر الإلكتروني لما يحققه من مزايا. وعلى الرغم من ذلك فإن النشر الإلكتروني في الجامعات العربية يواجه صعوبات لعل أهمها:

– عدم وجود قوانين تضمن حماية حقوق المؤلفين.

– عدم اعتراف اللجان الأكاديمية ولجان الترقيات بالأبحاث المنشورة على الإنترنت؛ لذا فإن الباحثين يترددون في تقديم بحوثهم للنشر في الدوريات الإلكترونية ويفضلون الدوريات الورقية[7].

2- **مفهوم المكتبة الرقمية:** إن الحديث عن المكتبات الرقمية قديم جداً حيث سبق وجود الحاسب الآلي بشكل تجاري، إلا أنها كانت متوقعة كنظام يوفر السرعة والسهولة في الوصول إلى المجموعات المكتبية من كتب ومواد.

وهناك من عرفها بأنها مجموعة من المعلومات الإلكترونية منظمة للاستخدام على المدى الطويل. وقد ذكرت منى الشيخ تعريفاً علمياً للمكتبة الرقمية تقترح من خلاله أن نفترض أن المكتبة الرقمية هي مكتبة تقليدية من حيث المفهوم والأداء والأهداف ومن حيث المهمات المكلفة بها من اقتناء المجاميع وحفظها وتطويرها والتحليل الموضوعي لها وإعداد الببليوغرافيات والكشافات وخزن واسترجاع المعلومات والخدمات المرجعية الأخرى وخدمات المستفيدين بشكل عام[8]، وتتم كل هذه العمليات بطريقة آلية.

إن تأسيس أو بناء مكتبة رقمية يطرح تحديات جدية، لأن تحويل المواد التقليدية إلى مواد رقمية لن يكون بالأمر السهل والمباشر، إذن لكي ننشئ مكتبة رقمية لابد من توفر بعض المكونات والاحتياجات وهي:

• انتقاء المعلومات التي يمكن بثها.

• إدخال المعلومات بأشكال مختلفة، بمعنى أن يكون قادراً على التعامل مع أوعية المعلومات شكلاً ومضموناً.

• مهارات في نظم الاسترجاع، وهي ذات أبعاد تكنولوجية وموضوعية في آن واحد.

وبإمكان المكتبات الرقمية أن تؤدي دورا مهما في الاستجابة للاحتياجات التعليمية المتزايدة وذلك بإعداد الأدلة حول الجامعات ومؤسسات التعليم العالي التي تتيح إمكانية التعلم عن بعد.

إن إنشاء المكتبات الرقمية ليس هدفا في حد ذاته، وإنما تفيد هذه المكتبات في إدارة المصادر الرقمية، والتجارة الإلكترونية، والنشر الإلكتروني، والتدريس والتعلم وغيرها من الأنشطة بوصفها أداة رئيسة في توصيل المحتوى لأجل أغراض البحث العلمي، والعمل التجاري، والحفاظ على التراث الثقافي والتعريف به.

3- مشاكل النشر الإلكتروني: يواجه النشر الإلكتروني عده مشاكل[9] أهمها:

- **انتهاكات حقوق الملكية الفكرية للناشرين والمؤلفين:** وتعتبر هذه أكبر مشكله تواجه النشر الإلكتروني لسهوله نسخ المحتوى الإلكتروني مقارنة بالكتاب الورقي وعدم وجود ضوابط تحكم القرصنة على شبكة الأنترنت ،حيث يتم نشر المحتوى المسروق بدون الرجوع للمؤلف. وقد بدأ ظهور تقنيات جديدة للحماية الإلكترونية للمحتوى على أقراص الليزر ومن خلال شبكة الأنترنت وتحدد ترخيص الاستخدام لشخص واحد وعلى جهاز واحد. هذا بالإضافة إلى التحرك على مستوى الشركات وجمعيات المجتمع المدني والحكومات للتصدي لظاهرة القرصنة. ونعتقد أن للإعلام وأنظمة التعليم دور كبير في نشر وتأصيل ثقافة احترام حقوق الملكية الفكرية.

- **ضرورة توفر أجهزة لاستخدام المحتوى الإلكتروني:** مثل جهاز الكمبيوتر أو جهاز الكتاب الإلكتروني أو الموبيل بينما الكتاب الورقي لا يحتاج إلا اقتنائه. ولكن هذه الأجهزة انتشرت الآن انتشارا كبيرا ولها استخدامات كثيرة ومتعددة ليست قاصرة على استخدامات الكتاب الإلكتروني.

- **صعوبة القراءة من الشاشة للأجهزة الإلكترونية:** فهي بلا شك غير مريحة للعين مثل الكتاب الورقي بالإضافة إلى أنها لا تعوض متعه القراءة من الكتاب الورقي. إلا أن الجيل الجديد لا توجد لديه هذه المشكلة بالإضافة لتطور أنواع

الشاشات وتقنياتها، ووجود إمكانيات الطباعة للمحتوى الإلكتروني للتمتع بالقراءة من الورق.

ثانيا: الوصول الحر للمعلومات: إن الوصول الحر للمعلومات هو جعل المحتوى المعلوماتي حراً ومتاحا عالميا عبر شبكة الانترنت، حيث أن الناشر يحفظ أرشيفات على الخط المباشر يتاح الوصول إليها مجانا، أو أنه يودع المعلومات في مستودع مفتوح الوصول ومتاح على نطاق واسع. والوصول الحر يعد نمط جديد للنشر العلمي نشأ لتحرير الباحثين والمكتبات من القيود المفروضة عليها.[10]

ويعرف "وحيد قدورة" الوصول الحر بأنه: "تكريس لمبدأ مجانية الوصول إلى المنشورات العلمية للتصدي للارتفاع المستمر لأسعار الدوريات العلمية، هذا على المستوى الاقتصادي، أما على المستوى الاتصالي فالمبدأ هو التداول السريع للمعلومات العلمية بين الباحثين والحصول على مرئيات أفضل للأدبيات العلمية ومن هذا المنطلق يرد مفهوم الوصول الحر والذي يهدف إلى إتاحة المعلومات وإنشاء مكتبة عالمية قابلة للتبادل على الدوام[11].

وعرف معجم SCHOLARLYCOMMUNICATIONS GLOSSARY مصطلح الوصول الحر هو تلك المعلومات المتاحة في شكل رقمي ومجاني على الخط المباشر من خلال الاتفاقيات والتراخيص الحرة لحقوق الملكية الفكرية.[12]

وهناك طريقان رئيسان للوصول الحر:

– الطريق الذهبي: ويعني القيام بنشر دوريات علمية محكمة لا تهدف إلى الربح المادي، وتسمح للمستفيدين منها (دون أية رسوم) بالتمكن من الوصول عبر الإنترنت إلى النسخ الإلكترونية من المقالات التي تقوم بنشرها. وتنبغي الإشارة إلى أن هذا النمط من الدوريات يتمتع بالخصائص نفسها التي تتمتع بها الدوريات المقيدة ذات الرسوم، وعلى رأسها التحكيم العلمي للمقالات.

– الطريق الأخضر: ويعني قيام الدوريات القائمة على الربح المادي بالسماح وتشجيع إيداع المقالات المحكمة المنشورة بها (في نفس وقت النشر أو بعده بفترة قصيرة) في مستودعات متاحة على العموم على الخط المباشر.

ظهر جلياً مبدأ الوصول الحر للمعلومات وأخذ يتزايد ينمو شيئاً فشيئاً وأصبح مطلباً ملحاً للباحثين والمتخصصين لكي يسهل لهم الوصول إلى المعلومات ويمنحهم الفرصة للإفادة منها والبحث فيها دون أية قيود خاصة مع مصادقة الكونجرس الأمريكي على مشروع قانون Martin Sabo والمعروف بـــ Public Access to Science Act الذي ينص على إعفاء البحوث الممولة من طرف الحكومة الفيدرالية من قانون حقوق النشر، وهو ما سيجعلها متاحة مجاناً أم جمهور المستفيدين.[13]

وهكذا أصبحت الفائدة المرجوة من مبدأ الوصول الحر في الوقت الراهن وعلى المدى الطويل مرتبطة ارتباطاً وثيقاً بالأهداف المرجو تحقيقها من البحث العلمي ذاته[14].

وتكمن أهمية الوصول الحر للمعلومات في قدرتها على تحقيق ثلاث أهداف وهي:

1ـــ ضمان وصول المستفيد، من خلال الاستعمال الأمثل للتكنولوجيات المتنوعة، إلى المعلومات العلمية والتقنية التي تلبي حاجياته، وهو ما يعني ضرورة إتاحة المعلومات الحرة على الشكل الإلكتروني.

2 ـــ استمرارية هذا الوصول، وهو ما يعني التمكن ليس فقط من رقمنته وأرشفته، بل من الاحتفاظ به واسترجاعه كلما دعت الضرورة.

3 ـــ مجانية هذا الوصول، أي انتفاء أي نوع من أنواع القيود، سواء منها المفروضة عن طريق حقوق التأليف أو عبر رخص الاستعمال الأخرى.[15]

يمكن بلورة مميزات الوصول الحر للمعلومات فيما يلي:

1ـ أن الوصول الحر للمعلومات يعد قوة جذب للباحثين ونظراً لأن المعلومات المتلقاة منها ذات قيمة شمولية بمعنى أنها تغطي مجالات الاهتمامات كافة من أهمها المعلومات العلمية والتكنولوجية، بالإضافة إلى أن الشمولية تعنى عرض المعلومات بصورة متكاملة تظهر معها مختلف وجهات النظر التي تتناول الموضوع مما يضفى قيمة مضافة وفائدة كبيرة على متلقي المعلومة حيث تعرض عليه الآراء المختلفة كافة مما يضيف عمقاً على المعلومات المتلقاة.

2ـ سهولة ومشروعية التعامل مع مصادر الوصول الحر دون أي قيود تعيق الاستخدام المشروع حيث أن مصادر الوصول الحر تتسم بأنها متاحة لجمهور المستفيدين مجاناً.

3 ـ مصادر الوصول الحر تتسم أيضاً بالتحديث المستمر للمعلومات مما يزيد بعداً آخر من الاستفادة منها في كافة المجالات ولاسيما التي تتسم بالتطور السريع والمتلاحق. وهذا يضمن استمرارية بقاء مصادر الوصول الحر وندرة توقفها.

ويضيف" كمال بوكرزازة" إلى هذه المزايا:

1ـ كسر احتكار الناشرين فيما يتعلق بتوزيع البحث العلمي، حيث إنه يجعل الوصول للمعلومات العلمية والتقنية أكثر عدلا وإنصافا.

2 ـ يتيح للمؤلفين الاحتفاظ بحق النشر، والبث المتزايد لأعمالهم على نطاق واسع.

3 ـ تسريع وتيرة البحث العلمي والتقني، إذ أن هذا النظام يسمح بالتخفيض في آجال نشر المقالات من 12 شهراً في المتوسط إلى بضعة أسابيع أو حتى بضعة أيام.

4 ـ تقوية الإنتاجية العلمية.

5 ـ تقوية التواصل بين الباحثين من مختلف التوجهات.[16]

وهذه المزايا لا تمنع من وجود بعض العيوب أو المشكلات التي تقف أمام الباحثين اتجاه الوصول الحر للمعلومات، ومن هذه المشكلات:

1 ــ عدم توفر الدراية الكافية لدى الكثير من الباحثين نحو استخدام أدوات البحث الملائمة لتحقيق الوصول للمواد التي تخدم بالفعل الحاجة البحثية.

2 ــ اضطراب الباحث وحيرته أمام توافر كم هائل من المواد المستدعاة، وعدم قدرته على التمييز بين المواد أو النتائج ذات الصلة بموضوع بحثه، والنتائج التي لا تضيف له جديدا أو ربما تكون بعيدة الصلة عن موضوع البحث، مما يترتب عليه ضياع الكثير من الوقت في عملية التصفح، والتحقق من المواد ذات الصلة بموضوع بحثه.

3 ــ عدم الوصول في كل الأحوال للنصوص الكاملة.

4 ــ مدى صحة ومصداقية المعلومات المتاحة من خلال الإنترنت، ومدى قدرة الباحث على التمييز ما بين الغث والثمين من المواد المتاحة.

5 ــ ليست كل الوثائق متاحة بالفعل في الشكل الإلكتروني.

6 ــ التغير الدائم في عناوين العديد من المواقع الإلكترونية ومن ثم ربما لا يستطيع الباحث العودة مرة أخرى للحصول على المعلومات نفسها أو متابعة تحديثها.

7ــ الاختلاف والتغيير المستمر في المعلومات المتاحة يوما عن يوم عبر الإنترنت، مما ينعكس على صحة وجودة الاستشهاد المرجعية[17].

ومن بين المشروعات التي تستهدف الإتاحة الإلكترونية للرسائل الجامعية نذكر على سبيل المثال لا الحصر:

- **مشروعات على المستوى العالمي:**[18]

· الكشاف العالمي للنصوص الكاملة المجانية للرسائل الجامعية المتاحة ETD.

· المكتبة الرقمية الشبكية للرسائل الجامعية: The Networked Digital Library of Theses and Dissertations (NDLTD)

· دليل مبادرات الرسائل الجامعية الإلكترونية المتاحة تجارياً أو من خلال الجامعات: Electronic These and Dissertations Initiatives.

· البوابة الكندية للرسائل الجامعية: The Theses Canada Portal

· مركز أوهايو للرسائل الجامعية الإلكترونية: The OhioLINK ETD Center

· مؤسسة الرسائل الجامعية الهندية: Digital Dissertation Foundation, India.

هذا بالإضافة إلى الخدمة التجارية العالمية لشركة ProQuest ومجموعة اللوائح المنظمة لخدمات التصوير الورقي والاستنساخ الإلكتروني للمكتبات الجامعية الأجنبية والعربية.

ثالثا: سرقات الملكيات الفكرية:

1- مفهوم الملكية الفكرية: قد أتاحت الحرية المطلقة على الإنترنت للأفراد – سواء كان فرداً أو جماعة رسمية أو غير رسمية- سهولة إصدار أي موقع، وينشر عليه مواد منقولة من أي مصدر أو مرسلة من أي قارئ، دون التأكد من مصدرها ودون أي ضوابط للنشر.

والملكية الفكرية تعني سلطة تخول لشخص على شيء غير مادي (معنوي) وهو ما يتعلق بالفكر والنتاج الفكري وغير ذلك، وعرف مفهوم الملكية الفكرية بأنه حق الإنسان في إنتاجه العلمي والأدبي والفني والتقني ليستفيد من ثماره وآثاره المادية والمعنوية، وحرية التصرف فيها والتنازل عنها واستئثارها[19]. وعرف محمد الشلش الملكية الفكرية بأنها: "ثمرة الإبداع والاختراع سماها بعض القانونيين بالملكية الذهنية لأنها ترد على نتاج ذهني ومثالها حق المؤلف على مؤلفاته وحق المخترع على اختراعه وحق التاجر في علامته التجارية وغير ذلك"[20].

وهناك من يعرف الملكية الفكرية على أنها الحقوق التي يمنحها المجتمع إلى الأفراد أو المنظمات بصورة رئيسية للأعمال الإبداعية مثل الاختراعات والأعمال الأدبية والفنية والرموز، ويمكن تعريفها علي أنها الحقوق التي يمنحها المجتمع إلى الأفراد أو المنظمات بصورة رئيسية للأعمال الإبداعية مثل الاختراعات والأعمال الأدبية والفنية والرموز والأسماء والصور والتصميمات. فهي تعطي المبدع الحق

في منع الآخرين من استعمال إبداعاته استعمالا غير مصرح به لمدة محدودة من الوقت.[21]

2-**حقوق المؤلف في البيئة الرقمية:** حق المؤلف هو مصطلح قانوني يصف الحقوق الممنوحة للمبدعين في مصنفاتهم الأدبية والفنية، ويشمل المصنفات الأدبية وبرامج الحاسوب وقواعد البيانات والبرامج والأفلام والقطع الموسيقية وتصاميم الرقصات والمصنفات الفنية مثل اللوحات الزيتية، الرسوم، الصور الشمسية والمنحوتات ومصنفات الهندسة المعمارية والخرائط الجغرافية والرسوم التقنية تتمتع الحقوق المادية للمؤلف بالحماية طيلة مدة حياة المؤلف يضاف إليها مدة خمسين سنة[22] تسري اعتبارا من نهاية السنة التي حصلت فيها وفاة المؤلف أو آخر مؤلف في حالة الأعمال المشتركة. وتنقسم حقوق المؤلف إلى:

- **الحقوق المعنوية:** وتتمثل في الفكرة الابتكارية إلى الشخص المبتكر ونجملها في :

أ- الحق في أن ينسب إليه مصنفه وأن يذكر اسمه على جميع النسخ المنتجة.

ب- الحق في تقرير نشر مصنفه وفي تعيين طريقة النشر وموعده.

ج - الحق في إجراء أي تعديل على مصنفه سواء بالتغيير أو التنقيح أو الحذف أو الإضافة.

د - الحق في دفع أي اعتداء على مصنفه وفي منع أي تشويه أو تحريف أو أي تعديل آخر عليه أو أي مساس به من شأنه الإضرار بسمعته وشرفه على أنه إذا حصل أي حذف أو تغيير أو إضافة أو أي تعديل آخر في ترجمة المصنف.

هـ - الحق في سحب مصنفه من التداول إذا وجدت أسباب جدية ومشروعة لذلك ويلزم المؤلف في هذه الحالة بتعويض من آلت إليه حقوق الاستغلال المالي تعويضاً عادلاً .

- **الحقوق المادية:** هي الحق بالاستغلال المادي وتتمثل في الإفادة مالياً من الإنتاج الفكري والإبداعي، فهو حق مؤقت، ويجوز لمالك الحق بعد ذلك أن

يتصرف به كيفما يشاء، حيث أن للمؤلف الحق في استغلال مصنفه بأي طريقة يختارها ولا يجوز للغير القيام بأي تصرف مما هو مبين أدناه دون إذن كتابي من المؤلف أو من يخلفه ،وتتمثل الحقوق المادية فيما يلي:

أ .الحق في استنساخ المصنف بأي طريقة أو شكل سواء كان بصورة مؤقتة أو دائمة بما في ذلك التصوير الفوتوغرافي أو السينمائي أو التسجيل الرقمي الإلكتروني والحق في طباعة المصنف وإذاعته وإخراجه.

ب. الحق في ترجمة المصنف إلى لغة أخرى أو اقتباسه أو توزيعه موسيقيا أو إجراء أي تحوير عليه.

ج. الحق في التأجير التجاري للنسخة الأصلية من المصنف أو نسخة منه إلى الجمهور.

د. الحق في توزيع المصنف أو نسخه عن طريق البيع أو أي تصرف آخر ناقل للملكية.

هـ. الحق في استيراد نسخ من المصنف وان كانت هذه النسخ قد أعدت بموافقة صاحب الحق فيه.

والحق في نقل المصنف إلى الجمهور عن طريق التلاوة أو الإلقاء أو العرض أو التمثيل أو النشر الإذاعي أو التلفزيوني أو السينمائي أو أي وسيلة أخرى سلكية كانت أو لاسلكية بما في ذلك إتاحة هذا المصنف للجمهور بطريقة تمكنه من الوصول إليه في أي زمان ومكان يختاره أي منهم .

أما عن طرق التعدي وانتهاك حقوق المؤلف للمصنفات في **البيئة الرقمية** فهي كالتالي:

1 - نشر المصنف من قبل دور النشر الإلكترونية دون إذن المؤلف أو المتنازل إليه يعد تعدياً على حق المؤلف.

2- النسخ واللصق يعتبر تعدي على المصنف المحمي إعادة النسخ.

3- التعديل والتوزيع وإعادة التوزيع.

4- التحميل على أجهزة الحاسب والتوزيع والتحوير للمصنفات.

5 - التثبيت على الدعائم الالكترونية يعد نسخاً غير مشروع.

6 – مجرد نشر المصنف على شبكة الإنترنت دون ترخيص من صاحب الحق يعد تعدي...

3– **حق الملكية الفكرية للرسائل الجامعية في البيئة الرقمية:** لا توجد مشاكل كبيرة بالنسبة لحقوق النشر أو الملكية الفكرية في مجال المواد المطبوعة، فشراء المكتبة للنسخة المطبوعة يخولها لإعارتها لمن تريد وبأي عدد من المرات بدون الحصول على أي ترخيص من مالك حقوق النشر، كما أن المستفيد من المكتبة التقليدية يقوم باستعارة وعاء المعلومات من أجل القراءة والإطلاع ومن ثم يقوم بإعادته للمكتبة لتقوم هي بعد ذلك بإعارته لشخص آخر، بينما في المكتبة الرقمية فالأمر مختلف تماماً، فلا توجد هناك عملية استعارة أساساً فالمستفيد يقوم بعملية إنزال مصدر المعلومات الرقمي من موقع المكتبة على الشبكة مما يخوله لملكيته الكاملة، كما أن المكتبة تتيح أي عدد مهما بلغ من عمليات إنزال مصدر المعلومات الرقمي. ويخشى كثير من المهتمين بحماية حقوق النشر والملكية الفكرية في هذه الحالة من قيام هذا المستفيد أو غيره بأي عمل غير نظامي ربما ينتج عنه فقد معلومات المؤلف من مصدر المعلومات الرقمي، أو قد توضع بغير اسمه، كما أنه في بعض الأحيان ربما تظهر بيانات المؤلف صحيحة وسليمة ولكن قد يحدث تغيير في محتويات مصدر المعلومات الرقمي وذلك بإضافة أو حذف محتوياته بغير علم المؤلف ورغبته، والتي ربما تؤدي إلى ظهور اسم المؤلف على مادة أو أفكار تختلف مع معتقداته وقناعاته.[23]

أثبت الواقع العملي أن القوانين الوطنية ليس بمقدورها توفير الحماية الكافية للمصنفات التي تنشر في البيئة الرقمية، وكان لا بد من ابتكار وسائل تقنية لحماية المصنفات، بمعنى توفير الحماية للمصنفات بمعرفة أصحاب الحقوق أنفسهم باستخدام وسائل تكنولوجية (مثل التشفير)، ومن خلال هذه الوسائل يتمكن لأصحاب الحقوق السيطرة على مصنفاتهم ومنع الاعتداء عليها، وبالتالي أصبح من

الممكن استغلال هذه المصنفات عن طريق الترخيص للغير باستعمالها والحصول على عائد مالي مقابل ذلك والهدف من استخدام هذه الوسائل التقنية هو ما يلي:[24]

1 - منع الوصول إلى المصنف محل الحماية الموجود في البيئة الرقمية إلا بإذن أو ترخيص من صاحب حق المؤلف والحقوق المجاورة وذلك باستخدام تقنيات التشفير بمختلف أنواعها.

2 - وضع نظام لسداد المقابل إلكترونياً، في كل مرة يرغب فيها أي من مستخدمي الإنترنت، للوصول والاطلاع على المصنف محل الحماية.

3 - تدابير تمنع نسخ المصنف المحمي بدون ترخيص من صاحب حق المؤلف.

4 - حظر تصنيع أو بيع الأجهزة أو الخدمات التي تستعمل في التحايل على التدابير التكنولوجية المتقدمة بنوعيها.

الخاتمة: بناءً على ما تم تقديمه توصلنا إلى النتائج الآتية:

– تشجيع استخدام النشر الإلكتروني إثراء للمحتوى الرقمي العربي على شبكة الإنترنيت.

– إتاحة النفاذ الحر للمعلومات عن طريق التحول من المكتبة الجامعية التقليدية إلى المكتبة الرقمية ارتقاء بالبحث العلمي الأكاديمي.

–استثمار الرسائل والأطروحات الجامعية في بناء المحتوى الرقمي الجامعي تثمينا لجهود الطلبة الباحثين.

– العمل على وضع تشريعات وطنية وعربية لحماية حقوق الملكية الفكرية لأصحاب الرسائل المنشورة إلكترونيا؛ نظرا لأن التشريعات الخاصة بحقوق التأليف التقليدية لا تغطي كل الجوانب المتعلقة بالتعامل مع المعلومات والأوعية الإلكترونية.

– العمل على تشريع قوانين تحمي حقوق الملكية الفكرية للباحثين عند رغبتهم في نشر أبحاثهم من خلال المكتبات الإلكترونية.

– تكثيف الإعلام والتعريف بالمكتبة الرقمية لتشجيع المستفيدين على استخدامها مع ضرورة تدريبهم على استخدام مواردها الرقمية، وإعداد ورش العمل اللازمة وتقديم الاستشارات اللازمة للترغيب والتعريف بواقع الخدمات وتحقيق الفائدة المرجوة منها مع ضمان الحماية اللازمة للمحتوى الرقمي.

– التوعية بضرورة توفير كل الوسائل التقنية كالفهارس الآلية وغيرها للاتصال المباشر لكل مكتبة.

– تأمين برامج واستراتيجيات أمن المعلومات وصيانة البرمجيات والشبكات والتجهيزات الإلكترونية وتطويرها لحماية المحتوى الرقمي من كل التهديدات والمخاطر المتوقع حدوثها.

– نشر الوعي بحقوق المؤلف والحقوق المجاورة في البيئة الرقمية للمؤلفين ومستخدمي شبكة الإنترنت.

– تفعيل الحماية القانونية لحقوق الملكية الفكرية في البيئة الرقمية وإصدار قانون عربي يضمن هذه الحماية في البيئة الرقمية.

الهوامش

1- أيمن السامرائي وعامر قنديلجي "النشر المكتبي الإلكتروني" رسالة المكتبة، م30، ع 3 (أيلول 1995م) ص 38

2 – شوقي سالم، صناعة المعلومات: دراسة لمظاهر تقنية المعلومات المتطورة وآثارها على المنطقة العربية، الكويت، شركة المكتبات الكويتية، 1990م ص 227 – 229.

3 – سوسن زهير المهتدي، تكنولوجيا الحكومة الإلكترونية، دار أسامة للنشر والتوزيع، الأردن- عمان، الطبعة الأولى، 2011، ص 261.

4 – د. رضا سعيد مقبل كلية اللغة العربية بالمنوفية – جامعة الأزهر بحث قدم لمؤتمر حركة نشر الكتب في مصر – المجلس الأعلى للثقافة، (11-13 مايو، 2009 ص19).

5 – حسن أبو خضرة – النشر الإلكتروني – رسالة المكتبة 23 (3) أيلول 1988م ص 24.

6 – سليمان الميمان: استثمار الإنترنت في الدعوة إلى الله، ورقة عمل مقدمة لندوة الكتاب الإلكتروني المصاحب لمعرض الكتاب الإلكتروني – المنعقد في مركز الملك فيصل للبحوث والدراسات الإسلامية – 21-30 / 12 / 1420هـ

7- حشمت قاسم. الدوريات الالكترونية المتخصصة: تطورها وتحدياتها الاجتماعية والاقتصادية .- مجلة مكتبة الملك فهد .- مج9 ، ع2 (رجب – ذو الحجة ،1424هـ) .- ص 277

8 – الشيخ، منى. المكتبة الرقمية D.L "المفهوم والتحدي"، المجلة العربية للمعلومات، إدارة التوثيق والمعلومات، المنظمة العربية للتربية والثقافة والعلوم، تونس، المجلد21، العدد الأول، 2000م، ص88.

9 – سوسن زهير المهتدي، تكنولوجيا الحكومة الإلكترونية، ص287.

10- Reitz, Joan M. Dictionary for library and information science.- Westport, Conn. : Libraries Unlimited, 2004.- p.501.

11 – وحيد قدورة. الاتصال العلمي والوصول الحر للمعلومات العلمية.– مصدر سابق. ــ ص .168

12 - Guide to the Open Access Movement Accessed26/12/2008 **Available on**: http://www❙earlham.edu/~peters /fos /guide.htm

13 - Willinsky,J. The access principle: the case for open access to research and scholarship Cambridge, MA: MIT.2006

14- HARNAD, Stevan .Open access publishing raises questions. ***Neuroscience Quarterly*** Accessed 22/7/2008 **Available on** http://www.sfn.org/?pagename=neuroscienceQuarterly_06winter_main

15- Peter, Suber. A very brief introduction to open accessAccessed26/9/2008**Available on:**www.Earlham.edu/~peters/fos/brief/.htm

16– بوكرزازة، كمال. الدوريات الإلكترونية العلمية بالمكتبات الجامعية وأثرها على الدوريات الورقية (2. ***Cybrarians journal***. - (ع11(ديسمبر 2006 Accessed26/9/2008**Available on:** www.cybrarians.info/journal/no ll/ejournals.htm

17 – المرجع نفسه

18 – أ.د. شريف كامل شاهين، الملكية الفكرية في بيئة التعلم الإلكتروني: نحو مبادرة للإتاحة المجانية للكتب الدراسية Open Textbooks في الجامعات المصرية على شبكة الإنترنت: جامعة القاهرة أستاذ ورئيس قسم المكتبات والوثائق وتقنية المعلومات، جامعة القاهرة، مدير المكتبة المركزية الجديدة للجامعة، sherifshn@yahoo.com موذجاً، العدد 27، ديسمبر 2011

19 – لإسلام والملكية الفكرية الشيخ محمد عثمان بشير أستاذ الفقه بجامعة قطر مقال منشور على موقع هندسة عربي الدراسات الإسلامية April 30, 2011 - 4:00

20 – حقوق الملكية الفكرية بين الفقه والقانون لمحمد الشلش جامعة القدس منشور على موقع جامعة النجاح الوطنية.

21 – أ.د. شريف كامل شاهين، الملكية الفكرية في بيئة التعلم الإلكتروني، المرجع السابق.

22 – غالب شنيكات. حقوق المؤلف في البيئة الرقمية والنشر الالكتروني.– (مارس 2007 -. <21>متاح في http://www.arab-ewriters.com/?action=showitem&&id=3343

23 – يونس عرب. التدابير التشريعية العربية كحماية المعلومات والمصنفات الرقمية.– مجله العربية– النادي العربي للمعلومات <21> -. متاح في-http:// www.arabcin.net/arabiaall/1 2003/5.html

24 – المرجع نفسه.

مفهوم الأمن المعلوماتي وواقع الجريمة الإلكترونية في مذكرات طلبة السنة الثالثة ليسانس ل.م.د قسم اللغة العربية وآدابها جامعة منتوري قسنطينة أنموذجا

أ. شيماء دراجي

مقدمة: يشكل الانترنت قفزة نوعية وأهم اختراع اخترعته البشرية، فالشبكة العالمية للانترنت تنقل كمية كبيرة من المعلومات في جميع المجالات فهي أداة قيمة بشكل غير معقول للبحث وجمع المعلومات عن الشركات المنافسة في المناطق المختلفة من العالم أو البحث عن معلومات أو إدراج المعلومات لتمكين الآخرين منها، فشبكة الانترنت سهلت عملية الاتصال بين مجموعة من الحاسبات الآلية بالإضافة إلى فوائد جمة للشبكة فهي تضم أفضل أنواع التواصل والتي يجب استخدامها في شتى مجالات الحياة، ولكن قليلون منا يعلمون بشأن مخاطر الانترنت مما جعل الجرائم المنظمة تقوم بتأسيس نفسها على الشبكة الكبيرة، ومن الممكن أن يقوم حوالي خمسة أو عشرة أشخاص بأن يلحقوا أضرارا أكبر من جيش وبكامل عتاده ومؤلف من مائة ألف عضو عندها كأنك تحمل قنبلة بين يديك ومن دون التمكن من تعطيلها، إن استخدام الانترنت أصبح كاستخدام سلاح ذي حدين.

ومنذ زمن بعيد بدأت تتعرض إلى أشكال مستحدثة من الاعتداءات بواسطة هذه التقنية الحديثة فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية بشتى أنواعها أو النصب، وكانت الثقة في المحررات الورقية يعتدى عليها بواسطة التزوير، أصبحت هذه الخصوصيات والممتلكات والمعلومات يعتدي عليها عن

طريق اختراق الشبكات المعلوماتية وإجراء التحويلات الإلكترونية من أقصى مشارق الأرض الى مغاربها في لحظات معدودة، كاختراق البريد الالكتروني والحواسب الشخصية، وقواعد البيانات الخاصة بالتأمين الصحي والمستشفيات ومؤسسات الائتمان والتأمين الاجتماعي كما أصبحت تلك الحقوق الثابتة في الأوعية الورقية يتم الاعتداء عليها في أوعيتها الإلكترونية المستحدثة عن طريق اختراق الشبكات والأنظمة المعلوماتية دون الحاجة إلى المساس بأي وثائق أو محررات ورقية.

وتعد السرقة العلمية من أبرز الاعتداءات بهذه التقنية الحديثة وكذلك من المشاكل الأخلاقية المعقدة والمتعددة الوجوه في المحيط الجامعي، ويمكن تعريفها على أنها تحدث عندما يقوم الكاتب متعمداً باستخدام كلمات أو أفكار أو معلومات «ليست عامة» خاصة بشخص آخر دون تعريف أو ذكر هذا الشخص أو مصدر هذه الكلمات أو المعلومات، ناسبها إلى نفسه. أو ما يسمى بالسطو على الملكية الفردية وهذا التعريف ينطبق على الكتابات المنشورة ورقياً أو إلكترونياً، أو الخاصة بطلاب آخرين. ومن أكثر أسباب اللجوء للسرقة العلمية: قصر الوقت وتأجيل إنجاز المهام إلى أن يحل الموعد النهائي لتسليم البحث، أو صعوبة البحث المطلوب، أو اعتياد الطلبة القيام بهذا العمل أو عدم وضوح مفهوم السطو على الملكية الفكرية والطريقة الصحيحة للاستشهاد والاقتباس.

والأسئلة الأساس التي عليها مدار المداخلة هي: ما مفهوم **الجريمة الإلكترونية والأمن المعلوماتي؟ وما هو واقع الجريمة الإلكترونية في مذكرات طلبة السنة الثالثة ليسانس ل.م.د؟**

1- تعريف الانترنت: يمكن تعريف الانترنت بأنها شبكة اتصالات عالمية تربط بين عدد من الحاسبات الآلية إما عن طريق خطوط هاتف أو عن طريق الأقمار الصناعية في جميع أنحاء العالم وعلى مدار الساعة.

كما يمكن تعريف الانترنت أيضا هي عبارة عن: "**اتصال بين مجموعة من الحاسبات الآلية الكمبيوتر من خلال شبكة اتصال متعددة أو أي وسيط اتقل للمعلومات التي يتشارك فيها المنظمات والمؤسسات الحكومية وغير الحكومية والافراد الذين قرروا السماح لآخرين بالاتصال بحواسبهم ومشاركتهم المعلومات**".[1]"

وذهب بعض الآخر إلى تعريفها بالنظر إلى خدماتها بأنها من وسائل الاتصال المسموعة والمرئية في آن واحد من وسائل اتصال عن بعد لأنها شبكة دولية تعمل بفصل البنية التحتية للاتصالات عن بعد."[2]"

وتعرف أيضا: هي عبارة عن شبكة حواسيب ضخمة متصلة مع بعضها بعض ويستخدم الانترنت أكثر من مليار مستخدم وكما تمكننا الانترنت من القيام بعديد من الأعمال بتصفح المواقع وجلب الأخبار المحلية والعالمية..."[3]".

2- مراحل تطور الانترنت: لقد مرت حياة البشر عبر مختلف الأزمنة بعدة تطورات ومراحل واكتشافات مست جميع مجالات نمط الحياة وتعد شبكة الانترنت جزء لا يتجزأ من هذه التطورات والاكتشافات الحاصلة، نشأت بدءا في القارة الأمريكية تحديدا الولايات المتحدة الأمريكية في السيتينيات على أسس وجذور عسكرية وعلمية بين وزارة الدفاع والجامعات الأمريكية هدفها أساسا تأمين اتصال لا يمكن قطعها.

إذ يعتبر الانترنت الذي بدأ العمل به في 1967 م شبكة لا مركزية تدعى إربانات إذ ربطت هذه الشبكة مجموعة من الجامعات الامريكية عبر أربع عقد مكونة من أجهزة الكمبيوتر عملاقة عندما كونت وزارة الدفاع الأمريكية فريقا بحثيا من العمل بمشروع بحثي كان موضوعه تشبيك الحاسبات لضمان استمرارية الاتصالات في حالة حدوث هجوم نووي"[4]".

في عام 1984، أعلن رسميا عن قيام شبكة الانترنت وذلك باتصال خمس شبكات ولم يقف الأمر إلى هذا الحد، بل وبسرعة فائقة انظمت شبكات أخرى

عديدة إليها منها ما هو محلي ومنها ما هو دولي كالشبكات العائدة للدول التي تدخل للدول مع الولايات المتحدة الأمريكية باتفاقيات خاصة حول الاتصالات "5".

في عام 1990 شهدت شبكة الانترنت ظهور شبكة أخرى إليها عظمت من قدراتها في الإمكانيات وزودتها بالصوت والصورة وأدوات الاعلام المتقدمة شبكة الواب.

حاليا لا يوجد أحد يملك الانترنت أو يسيطر عليها وإنما، هي ملكية تعاونية للبشرية جميعا بقدر اسهامهم فيها، فلا يوجد إدارة مركزية للانترنت وكل ما يمكن قوله في البداية كانت وزارة الدفاع الامريكية ثم المؤسسة القومية للعلوم الأمريكية هي المالك الوحيد للشبكة لكن بعد تطور الشبكة ونموها اختلف مفهوم التملك ليحل محله مجمع الانترنت الافتراضي كما أن تمويل الشبكة تحول من القطاع الحكومي إلى القطاع الخاص."6".

أما عن مشرعنا الجزائري ولأول مرة نظم الانترنت كنشاط اقتصادي مقنن بموجب المرسوم التنفيذي 283-257 المؤرخ في 25 أوت 1998 م الذي يضبط كيفيات إقامة خدمات الانترنت واستغلالها، من الناحية الشكلية عدد الحيثيات أو عدد النصوص التي استند عليها هذا القانون وهي ثلاثة عشرة يلاحظ من خلال غياب قانون المتعلق بترقية الاستثمار ويعتبر القانون مهما في هذه المرحلة وهي مرحلة الانتقال من اقصاد الموجه إلى الاقتصاد الحر ويتضمن هذا النص القانوني المتعلق بالانترنت 18 مادة، المادة الاولى منه تحديد شروط وكيفيات إقامة واستغلال خدمات الانترنت"7"

ونظرا للثورة التكنولوجية التي شهدها العالم، وهذه الثورة التي تمس تكنولوجيات والإعلام والاتصال (المعلوماتية ووسائل الاتصال الحديثة)، هذه التغيرات ادت إلى خلق مصطلح جديد يسمى الإجرام المعلوماتي بحيث الجريمة تقع على المعلومة"8" بمعناها المعلوماتي، (معطيات) برامج وله من وجود منطقي في النظام المعلوماتي، أي معالجتها نشرها واستعمالها غير مشروع.

فالجريمة المعلوماتية من أكبر التحديات التي نواجهها في عالمنا المعاصر لأنها تصنف من الجرائم الحديثة التي تتخذ القواعد التقليدية للتجريم والعقاب التي تقتضي ضرورة تحقق أركان الجريمة طبقا لمبدأ شرعية الجرائم والعقوبات. لأنها أثارت خلافا في الأوساط الفقهية بخصوص تحديد ماهيتها والأفعال التي تدخل في نطاقها ،فلا يوجد مصطلح موحد للدلالة على الجرائم المرتبطة بالإعلام الآلي حيث اختلفت الاجتهادات لذلك اختلافا كبيرا، يرجع على سرعة وتيرة تطور تقنية المعلوماتية من جهة وتباين طور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فالنظام المعلوماتي لهذه التقنية يكون محلا للجريمة تارة ويكون لوسيلة لارتكابها تارة أخرى فالبعض يطلق عليها الغش المعلوماتي وآخرون ينعتونها بجرائم التكنولوجيا والبعض الآخر يطلق عليها تسمية الجريمة المعلوماتية مما يصعب معه الإقرار بوجوب تعريف موحد باعتبار أن هذه الظاهرة حديثة نسبيا.

1- تعريف الجريمة الالكترونية: لقد تباينت الآراء الفقهية لتعريف الجريمة الإلكترونية فهي متفاوتة فيما بينها ضيقا واتساعا ويمكن بوجه عام تصنيفها إلى أربع فئات التالية: "9"



شكل : 01 يبين تصنيف انواع الجرمة

1-1- تعريفات مرتكزة على موضوع الجريمة: نماذجها عديدة ومتباينة في تصورها لدور الحاسب الآلي في ارتكاب الجريمة فالجريمة المعلوماتية عند الفقيه الألماني تيدمان هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب.

ويعرفها مكتب التقنية في الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب: "**الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا أساسيا**".

وقريبا من هذا التعريف لليزلي بال للجريمة المرتبطة للحاسوب بأنها: "**فعل اجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية**".

وبعبارات تغلب عليها الطابع التقني يعرف كلا من **تيرزي وهاند كاستل** الجرائم المعلوماتية، من خلال تعريفها للجرائم المرتبطة أو المتعلقة بالحاسب بأنها: "**تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل**

نظام الحاسب وبعبارات أخرى هي تلك الجرائم التي يكون فيها دور الحاسب فيها ايجابيا".

الاعتماد في تعريف الجريمة الالكترونية على الوسيلة المستخدمة في ارتكابها يوجه إليها نقذ مفاده أنه لكي تعرف الجريمة يجب الرجوع إلى العمل الاساسي المكون لها وليس فحسب الوسائل المستخدمة لتحقيقها.

1-2- تعريفات مرتكزة على موضوع الجريمة: الجريمة المعلوماتية (التكنولوجية) في منطق واضعي هذه التعريفات ليست هي التي يكون الحاسب أداة ارتكابها بل التي تقع على الحاسب أو داخل نظامه، ومن نماذج مسايرة هذا المنطق **روزن بالت وخبراء آخرين**، جريمة الحاسب بأنها نشاط غير مشروع موجه للنسخ أو تغيير حذف او الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه.

1-3- تعريفات مرتبطة بتوافر المعرفة بتقنيات المعلومات: ومن قبيلها تعريف **دافيد تومبسون** لجريمة الحاسب بأنها: "**أية جريمة يكون متطلبا لاقترافها أن تتواضع لدى فاعلها معرفة بتقنية الحاسب**".

واستخدام **سولراز** للدلالة على أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان كرتبط بتقنية المعلومات.

1-4- **تعريفات مختلطة ومتنوعة:**

من نماذج هذه التعريفات، القول بأن مصطلح "**جريمة الحاسب**" يشير بوجه عام إلى جريمة التي تمد معرفة للحاسب شرطا ضروريا أو استخدامه شرطا ضروريا لارتكابها والقول كذلك أن ما يسمى بجريمة الحاسب يتضمن تقريبا أي ضرر من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسب.

ويتبنى بعض تعريفا للجريمة المعلوماتية اقترحته مجموعة من منظمات تعاون الاقتصادي والتسمية كأساس للنقاش عقد في باريس سنة 1983 م للبحث في الاجرام المرتبط بالمعلوماتية، مقتضاه أنها: "كل سلوك غير شرعي أو غير

مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها، وهو تعريف يتسبب اتساعه البالغ كما يقوله بعض في تعليل نفعه للفقهاء.

أما المشرع الجزائري فهو لم يضع تعريفا للجريمة الإلكترونية إلا مؤخر من خلال المادة 2 فقرة1 من القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق ل 05-أوت 2009 المتضمن للقواعد الخاصة للوقاية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها".

وتجدر الإشارة إلى أن التعريف الذي ورد في القانون جاء عاما حيث اكتفى المشرع بتعريفها على أنها كل جرائم سواء المتعلقة بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي يرتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو أي نوع آخر من نظم الاتصال الإلكتروني حسب مضمون المادة 02 فقرة 01 السالفة للذكر ومن أجل تعريف شامل للجريمة الإلكترونية لابد من تعريفها من الجانب الفني أو التقني ومن الجانب القانوني.

ويمكن تعريفها من الجانب الفني بأنها: "**عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشر أو غير مباشرة كهدف أو وسيلة لتنفيذ الفعل الاجرامي**".

أما من الجانب القانوني فيمكن تعريفها بأنها: "مجموعة من الأفعال والأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الاجرامي والثورة التكنولوجية "["10"]

2- خصائص الجريمة الالكترونية: تتميز الجريمة الإلكترونية (المعلوماتية) بخصائص تميزها عن الجريمة التقليدية ولعل من اهمها ما يلي:

2-1- **الجريمة المعلوماتية جريمة عابرة للحدود:** الجريمة المعلوماتية تتميز غالبا بالطابع الدولي ذلك لأن الطابع العالمي لشبكة الانترنت وما يترتب من جعل معظم العالم في العالم في حالة اتصال دائم على الخط يسهل ارتكاب الجريمة من دولة إلى أخرى، فالجريمة المعلوماتية لا تعترف بالحدود بين الدول والقارات ولذلك فهي جريمة عابرة للقارات. فهي تعتبر شكلا جديدا من أشكال الجرائم

العابرة للحدود الإقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل جرائم التعدي على قواعد البيانات وتزوير واتلاف المستندات الالكترونية والاحتلال المعلوماتي وسرقة بطاقات الاءتمان والقرصنة وغسل الأموال.

والجريمة الإلكترونية هي نوع من الجرائم التي يتم ارتكابها عن بعد وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر الفاعل وبين النتيجة أي المعطيات محل الاعتداء، وبالتالي لا تقف الجريمة الالكترونية (المعلوماتية) عند الحدود الإقليمية لدولة معينة بل تمتد إلى الحدود الاقليمية لدولة أخرى"[11]"

2-2- **صعوبة الإثبات في مجال الجريمة المعلوماتية:** نظرا للطابع الخاص الذي تتميز به هذه الجرائم فإن اثباتها يحيط به الكثير من الصعوبات والتي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا فالجرائم المعلوماتية لا عنف فيها لا سفك دماء ولا آثار اقتحام سرقة أموال مثلا، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات وليس لها اي أثر خارجي ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية "[12]"

2-3-عدم وجود مفهوم مشترك للجريمة المعلوماتية: من خصائصها عدم وجود مفهوم مشترك لماهية الجريمة المعلوماتية وعدم وجود تعريف قانوني موحد ويرجع السبب لعدم وجود تنسيق دولي في مجال الجريمة المعلوماتية.

وقد اختلف الفكر القانوني حول حماية المعلومات فيرى بعص أن المعلومات لها طبيعة خاصة ولا يطبق عليها الشرط الضروري لتعريف الجريمة.

2-4- وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات: من خصائص الجريمة المعلوماتية قد تقع اثناء العملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة اخراج المعلومات.

2-5- قلة الابلاغ عن وقوع جرائم الانترنت: لا يتم الابلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها إما خشية من التشهير لذا نجد معظم جرائم الانترنت تم اكتشافها بالمصادقة بل وبعد وقت طويل من ارتكابها إذ توجد فجوة بين عدد هذه الجرائم الحقيقة وبين ما تم اكتشافها.

2-6- **الجريمة المعلوماتية جريمة مستحدثة:** تعد الجرائم الإلكترونية من أبرز الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة فلا غرابة أن تعتبر الجرائم المعلوماتية إساءة التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم امستحدثة كجرائم غسل الأموال تهريب المخدرات، اختراق قطاع الأعمال الإفلاس بالتدليس والغش والفساد سرقة الملكية الفكرية"[13].

ومن هذا المنطلق تعتبر الجريمة المعلوماتية من أكبر التحديات التي نواجهها في عالمنا المعاصر، إن لم تكن أكبرها على الاطلاق ولذا تتحضر القوى الكبرى في العالم للحرب الحاسوبية من خلال تجنيد أجهزتها الاستخبارية والأمنية لقراصنة حواسيب.

3- تعريف الأمن المعلوماتي: تتعدد تعريفات أمن المعلومات وتتنوع حسب زاوية الرؤية، فنحن إذا نظرنا من زاوية أكاديمية سنجد أنه العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

ولو نظرنا من زاوية تكنولوجية وفنية بحتة يمكننا تعريفه على أنه (الوسائل والأدوات والإجراءات المطلوب توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية)"[14]"، ومن الزاوية القانونية نجد التعريف قد أخذ منحى آخر لكونه يركز على التدابير والإجراءات التى من شأنها حماية سرية وسلامة وخصوصية محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها فى ارتكاب الجريمة المعلوماتية.

وبشكل عام يمكن القول أن أمن المعلومات هو تلك الرؤى والسياسات والإجراءات التى تصمم وتنفذ على مستويات مختلفة، فردية ومؤسسية ومجتمعية

وتستهدف تحقيق عناصر الحماية والصيانة المختلفة التي تضمن أن تتحقق للمعلومات السرية أو الموثوقية، أي التأكد من أن المعلومات لا تُكشف ولا يُطَّلع عليها من قبل أشخاص غير مخولين بذلك. أي التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشروع. أما الاستمرارية فتعني توفر وإتاحة المعلومات أو الخدمات المبنية عليها لمستخدميها والمستفيدين منها والتأكد من استمرار توفرها والنظم التي تخدمها واستمرار القدرة على التفاعل معها والتأكيد كذلك على أن مستخدمها لن يتعرض إلى منع الاستخدام أو الحيلولة بينه وبين الدخول إليها، كما تعني أيضا ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه هو الذي قام بهذا التصرف"[15].

2- أهمية امن المعلومات: للمعلومات أهمية وقيمة مادية ومعنوية للأفراد والشركات والدول، تزداد أهميتها في المنظمات الأمنية والعسكرية والاقتصادية ذات الطابع الاستراتيجي، لذلك ارتبط عنصر السرية بالمعلومات ودرجة توافرها من مكاسب حيث تلعب دورا كبيرا في انتصار أو هزيمة الدول.

1 - الحاجة للارتباط ينظم الاتصالات والانترنت، وعدم امكانية عزل أجهزة عن الشابكات المحلية والشبكات واسعة النطاق لتوفير المعلومات لمن يحتاجها

2- اعتماد مختلف المنظمات على فاعلية المعلومات

3ظهور التجارة الالكترونية والحكومة الالكترونية والادارة الالكترونية التي تحتاج الى بينى معلوماتية آمنة

3-صعوبة تحديد الأخطار والتحكم بها او متابعة المجرمين ومعاقبتهم لعدم توافر حدود جغرافية عند استخدام الانترنت والاتصالت الالكترونية لانها تتيح الفرصة لاختراق الحدود المكانية.

خريطة مفاهيمية تبين أهمية الأمن المعلوماتي

4- **تعريف السرقة العلمية:**"16" تعتبر السرقات العلمية نوع من أنواع الجرائم الإلكترونية فالسرقات الفكرية هي اغتصاب فكري النتاج العقلي أيا كان نوعية "أدبيا، علميا وعاما" ونشره دون الإشارة على مصدره الأصلي وتتعد أنواعها بتعدد المجالات الإبداعية كمجال الأدبي من شعر ونثر والمجال العلمي كالبحوث المنهجية والمجال العام وهو الكتابة فيما يخص مختلف القضايا كما تتفرع في درجة خطورتها على أنواع.

فهناك السرقة الفكرية التامة وهي قيام السارق بنقل الإنتاج الفكري كاملا ونسبته لنفسه وهناك السرقة الجزئية وهي الاستيلاء على جزء من مؤلف ما والاستعانة به لتكملة مؤلف آخر والتغطية على صاحب النص الأصلي، وأمثلة ذلك أن يقوم السارق بنسبة بحث ما أو عمل أدبي لنفسه دون الإشارة لصاحبه سواء

كانت السرقة منصبة على كامل النص أو جزء منه كما هناك السرقة الفكرية غير المباشرة وهى التى تعنى الاستيلاء على الفكرة دون النص أو عن النتيجة العلمية دون صلب البحث وهي لا تقل بأي حال من الأحوال عن السرقة الفكرية المباشرة أو الصريحة من حيث خطورتها على الأمانة العلمية ومثالها سرقة نتيجة علمية وإضافتها لبحث وكذلك سرقة التشبيهات أو الصور البلاغية من الأعمال الأدبية الإبداعية وصياغتها فى قالب نصي مختلف.

والسرقات الفكرية تختلف عن الاعتداء على حق المؤلف وإن كان كل منهما يمثل اعتداء وجرما .. فالسرقة الفكرية تأتي من نسبة النتاج الفكري إلى شخص ما باعتباره مؤلفه .. أما الاعتداء على حق المؤلف فهو استغلال المؤلف الفكري فى النشر أو الإنتاج التسويقي دون الحصول على إذن صاحب العمل. ..

ومن هنا يتضح الفارق حيث يكون الاعتداء على حق المؤلف محافظا على نسبة العمل ذاته إلى صاحبه الأصلي بعكس السرقة الفكرية وفى واقع الأمر أن السرقات الفكرية ليست وليدة العصر الحديث وإنما هى ضاربة فى القدم .. ولكن تأتي كارثة العصر الحالي فى معيار انتشارها وذيوعها إلى حد يهدد النماء الثقافي بالذات فى المجتمع العربي الذى أصبح موصوما بتراجع غير طبيعى فى المجال الثقافي عامة إضافة إلى ذيوع السرقات التى تضرب ما تبقي من أثر ايجابي للأمة كلها.

وفور انتشار المنتديات والمجلات الإلكترونية على شبكة الانترنت استفحلت الظاهرة على نحو مدمر بحيث كادت أن تصبح هى الأصل بينما الأمانة الفكرية هى الاستثناء .. فالعشرات من رواد المنتديات ينقلون وينسبون لأنفسهم غالبية ما يجدون لأعمال تخص مبدعين معروفين أو مجهولين ويشاركون بها في منتدياتهم طلبا للمدح والتزلف في أغلب الأحيان، ومع تجاهل المشكلة من المجتمع الثقافي فهناك من يفعل ذلك بحسن نية لجهله بضرورة الإشارة لنقل الموضوع واسم مؤلفه وهو عيب الإدارات المختلفة التي لا تولى تلك القضية اهتمامها بالتوعية الكافية

فضلا على ردود أفعالهم البسيطة تجاه تلك السرقات إضافة إلى مناصرة بعض الإدارات بالمنتديات المختلفة لأعضائها رغم إثبات قيامهم بالسرقة وكان الأمانة الفكرية تعد ظرفا طارئا وتقليدا جديدا .

إن لصوص الكلمة والفكرة لا ينتهجون طريقة واحدة في انتهاك حقوق الملكية الفكرية للآخرين، بل طرق عديدة، ظاهرة وخفية، مباشرة وغير مباشرة، ساذجة وذكية, بل ربما نسمع عن طرق جديدة مستحدثة في ظل التقدم المتسارع في تكنولوجيا المعلومات والاتصالات ندرج فقط اهم أنواع السرقة العلمية:

5- أنواع السرقة العلمية :"[17]"

5-1 سرقة المادة بالكامل: إن أشنع أنواع السرقات العلمية على الإطلاق، هو قيام الباحث السارق بسرقة الكتاب أو البحث بكامله, وقد يظن البعض أن أحدًا لا يجرأ على ذلك، والحق غير ذلك، فقد تكرر كثيرًا قيام أحدهم بكتابة اسمه مكان اسم المؤلف الأصلي وإعادة طباعة الكتاب في دار جديدة وفي بلد أخرى، وبهذا أصبح للكاتب السارق كتابًا لم يكتب فيه كلمة واحدة اللهم إلا اسمه!

5-2 فقرات محشوة: ومن أهم صور السرقات المباشرة والمتعارف عليها؛ إدخال الكاتب فقرة أو عدة فقرات كاملة – من كاتب آخر – إلى النص، دون أن يذكر اسم الكاتب الأصلي, فقد يبدأ الكاتب السارق المقالة بفكرته وبكلامه وسرعان ما يحشر داخل مقالته عدة فقرات خلسة من كاتب آخر، بحيث تبدو للقارئ وكأنها من بات أفكار الكاتب.

5-3 تفكيك وإعادة تركيب: وأحيانًا يقوم السارق بتفكيك مقالة الكاتب الضحية ثم إعادة تركيبها بألفاظ، ومصطلحات مختلفة لإخفاء جريمته، فيغير كلمات وجمل مثل: "الوطن العربي "إلى "العالم العربي"، "صحيفة" إلى "جريدة"، "أسد" إلى "سبع" "ناقة " إلى جمل" .. وهكذا، ومن حسن حظ السارق أن اللغة العربية لغة ثرية يمكن أن تسعفه في إعادة تفكيك النص وتركيبه بمصطلحات أخرى ..

5-4 السرقة عن طريق الترجمة: نوع آخر من السرقات العلمية يقوم به لصوص الكلمة، وذلك بترجمة نص أجنبي – مقالاً كان أو بحثًا أو رواية – إلى لغة أخرى على أساس أنه عمل من إنتاجه وأنه ليس مترجمًا، وبذلك يأكل حق المؤلف الأصلي صاحب الفكرة الأصلية والمادة الأساسية.

لقد ظهر في المجتمع الأكاديمي (الجامعات ومؤسسات البحث العلمي) أكاديميون يسرقون أبحاث منشورة ومطبوعة في مجلات علمية دولية، ويقدمونها في الجامعة طلبًا للترقية أو الحصول على درجة علمية، وسرعان ما يُكتشف أن رسالة الدكتوراه لفلان أو إعلان ما هي إلا رسالة أجنبية مترجمة.

5-5 سرقة النقاط البحثية: وقد يقوم السارق بالسطو على نقطة بحثية أو مخطط مسجل لباحث آخر، فمعروف أن باحث الماجستير أو الدكتوراه يذهب أولاً إلى قسم شئون الدراسات العليا ويقوم بتسجيل النقطة البحثية والمخطط المزمع إعداده على هيئة بحث موسع، فيحدث في بعض الأحيان قيام باحث" قليل الأدب" بالسطو على هذه النقطة وتسجيلها في جامعة أخرى مع استخدام الرشوة لتمرير الموضوع حيث يُمنع إعادة تسجيل نقطة ما سُجلت في أي جامعة أخرى السارق في هذه الحالة، حيث يجب على المشرف منع الباحث من تناول نقطة بحثية سبق تسجيلها.

5-6 سرقة عناوين الكتب المشهورة : بعدما نجح الكتاب الشهير "لا تحزن" للشيخ الدكتور عائض القرني، ظهرت عدة مؤلفات تحمل نفس العنوان، وقد يحتال أحدهم حتى لا يُتهم بالسرقة فيجعل العنوان "لا تحزن.. إن الله معنا" بحيث تكون الجملة الأولى "لا تحزن" بالخط العريض الواضح، وتكون الأخرى "إنا الله معنا" بخط خفيف .



خريطة مفاهيمية تبين انواع السرقة العلمية

الدراسة التطبيقية: إن نشر البحوث العلمية على الشبكة العنكبوتية جعل السرقة العلمية أكثر سهولة من ذي قبل، وتسبب في ظهور ما يعرف بالسرقات الرقمية التي مست جميع مستويات التعليم الجامعي قبل التدرج وما بعد التدرج.

فالجانب النظري غير كاف وحكمنا يبقى ناقصا، ولكي تصبح نظرتنا ثنائية الجانب تطرقنا إلى الجانب التطبيقي والذي احصينا ووصفنا فيه واقع الجريمة الإلكترونية في مذكرات طلبة السنة الثالثة ليسانس ل.م.د، فقمنا بجمع عدة مذكرات لرسائل الماجستير والدكتوراه في شعبة اللغة العربية تخصص اللغويات منشورة في مواقع الشبكة الإلكترونية في سنة 2010، كما جمعنا عدة رسائل الليسانس

المنجزة سنة 2014م، وقمنا بإحصاء أنواع السرقة العلمية وأكتفينا بأربع أنواع بدءا من المقدمات إلى متون وخواتم المذكرات، معتمدة في ذلك على نوعين من الجداول، فالصنف الأول يبين نماذج أنواع السرقات في مذكرات الليسانس والصنف الثاني يبين تكرار أنواع السرقات وهذا للكشف عن النوع المستفحل للسرقة العلمية لدى طلبة الثالثة ليسانس وإعطاء بعض الأمثلة فقط نظرا لضيق الوقت وطبيعة المقال، وتوضح نوع السرقة من النص الأصلي إلى النص المسروق من عدة مذكرات، كما قمنا باستقراء وتحليل الجداول الإحصائية للسرقة في نماذج مذكرة الليسانس.

كما اعتمدنا على تقنية برنامج الورد الذي يحصي عدد الكلمات والفقرات في النص جمعنا عدد الكلمات والفقرات الموجودة في كل مذكرة لاستخرج النسبة المئوية المسروقة في ثلاث مذكرات ليسانس انموذجا. وسبب اختياري للفقرة لأنها تتضمن فكرة الرئيسية، فابتكرت طريقة وتعتمد جل برامج كشف السرقات العلمية على الأبحاث على الفقرات والكلمات الكلمة مثل برنامج "ithenticate".

وذلك بوضع أي بحث عليه، ليتمكن البرنامج من كشف كل ما تم نسخه أو سرقته من بحث آخر منشور في الشبكة العنكبوتية بالكلمات.

ويكشف 8 أنواع من السرقات وهى :"[18]"

1 – الكشف عن البحث الذي تم لصقه بالكامل دون تغيير أي حرف.

2 – الكشف عن البحث الذي تم تغيير النص الأصلي له فقط مع الاحتفاظ بمعناه.

3 - الكشف عن البحث الذي نسب له المعلومات دون ذكر أي مراجع من التي لها أحقية البحث.

4 - الكشف عن القص واللصق لبعض العبارات في فقرات معنية.

5 - الكشف عن الأبحاث التي يتم فيها تغيير الأعداد والنسب والأرقام.

6 - الكشف عن الأبحاث التي تم نقلها بالجملة في المعنى مع تغيير الفقرات.

7 - الكشف عن الأبحاث التي يعاد تغريدها مرة أخرى بمعنى عدم تغيير حرف بها.

8 - الكشف عن الأبحاث التي تم تغيير الجمل الأساسية بالبحث فقط مثل العنوان "كلمات البحث."

ومن هذا المنطلق اعتمدت الدراسة للكشف عن السرقة العلمية يدويا حاصرة مجال انواع السرقة العلمية لضيق الوقت وللسعر المرتفع لاقتناء برنامج "ithenticate كاشف السرقات العلمية على الأبحاث.

للوصول إلى نتائج دقيقة.

عينة الدراسة:

- عدد من رسائل الدكتوراه والماجستير الأصلية والمنشورة في الشبكة العنكبوتية لسنة 2010. 10
- عدد من مذكرات الليسانس التي تحتوي على السرقة العلمية لسنة 2 03
- **رمزت للرسائل الثلاث ب الأرقام: 01-02-03، وهذا حتى لا نكشف هوية الطلبة**
- **فوائد الدراسة:**

– الكشف عن الانتحال والسرقات العلمية وتدعيمها بنماذج من النص الأصلي ومن النص المسروق.

– الحصول على تقرير يوضح نسبة التطابق التام أو الجزئي للمذكرات.

– قدمت هذه الدراسة:

–أ/ النسب المئوية لأنواع السرقة في عناصر المذكرات.

–ب/التقرير العام للتشابه.

–ج/تتبع المحتوى للوصول إلى أصل المعلومة.

- **منهج الدراسة: اعتمدت هذه الدراسة على منهج وصفي واستعنت على تقنية الإحصاء والتحليل.**

1- نماذج لأنواع السرقة في مذكرات ليسانس 2014:

أنواع السرقة	النموذج الأصلي	النموذج المسروق
سرقة المادة بالكامل	وقد عني نحاة اللغة العربية بأجزائها المكونة لها، دون الاهتمام بها، فدرسوا الألفاظ المفردة صيغة ووظيفة، وفسروا ما يعتريها من تعبير في حروفها وحركاتها فأشبعوها تحليلا، وهذا يعني أن دراسة النحو كانت دراسة تحليلية تهتم إلى حد كبير بالجزئيات وتهمل التراكيب التي هي جوهر الدرس النحوي ص-أ-	وقد عني نحاة اللغة العربية بأجزائها المكونة لها، دونها اهتمام بها، فدرسوا الألفاظ المفردة صيغة ووظيفة، وفسروا ما يعتريها من تعبير في حروفها وحركاتها فأشبعوها تحليلا، وهذا يعني أن دراسة النحو كانت دراسة تحليلية تهتم إلى حد كبير بالجزئيات وتهمل التراكيب التي هي جوهر الدرس النحوي ص-أ-
سرقة المادة بالكامل	وبما أن المقاربة بالكفاءة هي نظام جديد حاولنا في بحثنا هذا أن نختار مهارة الإملاء باعتبارها مادة كغيرها من مواد التدريس وهذه المادة يجرى تدريسها منذ المرحلة الابتدائية لأن هذه الأخيرة هي المرحلة الأولى التي يتكون بها التلميذ. ص-ث-	وبما أن المقاربة بالكفاءة هي نظام جديد حاولنا في بحثنا هذا أن نختار مهارة الإملاء باعتبارها مادة كغيرها من مواد التدريس وهذه المادة يجرى تدريسها منذ المرحلة الابتدائية لأن هذه الأخيرة هي المرحلة الأولى التي يتكون بها التلميذ. ص-ب-
سرقة المادة بالكامل	تدريس قواعد اللغة العربية في الطور الثانوي-السنة ثانية ثانوي-عنوان	تدريس قواعد اللغة العربية في الطور الثانوي-السنة ثانية ثانوي-عنوان
تفكيك وإعادة تركيب	-3/ **طريقة حوسبة الكلمات:** يقوم التلاميذ بكتابة نص إملائي،	طريقة حوسبة الكلمات: يقوم الطلبة بكتابة قطعة إملائية، ثم

	ثم يصحح بوضع خط تحت الكلمة خطأ ا، ويتم تصويبها بإشراف المعلم. 2-4/ **حساب** الكلمات التي يخطئ فيها أغلب التلاميذ، وعرضها وتصويبها على السبورة ثم إعادة إملائها.ص 183 2-5/ كتابة كلمة يخطأ فيها أكثر التلاميذ في بطاقة بخط كبير وتعليقها فوق السبورة أسبوعا وتغييرها بكلمة أخرى في الأسبوع التالي. ص-208-	تصحح بوضع خط أحمر تحت الكلمة الخطأ، ويتم تصويبها بإشراف المعلم.. 2-4/ حصر الكلمات التي يخطئ فيها أغلب الطلبة، وعرضها وتصويبها على السبورة ثم إعادة إملائها. ص: 67 2-5/ كتابة كلمة يخطأ فيها أكثر التلاميذ في بطاقة بخط كبير وتعليقها فوق السبورة أسبوعا وتغييرها بكلمة أخرى في الأسبوع التالي. التالي. ص75
تفكيك وإعادة تركيب	إن الإملاء بوصفها مهارة يتعلمها المتعلم، لابد من إتقانها امتثالا لقول النبي صلى الله عليه وسلم:« **إن الله يحب إذا عمل أحدكم عملا أن يتقنه** » صدق رسول الله. ص-35	من المهارات التي يتعلمها التلميذ مهارة الإملاء لا بد من التمكن منها لقول النبي صلى الله عليه وسلم: "إن الله يحب إذا عمل أحدكم عملا أن يتقنه" صدق رسول الله ص-23
تفكيك وإعادة تركيب	ودراستنا لبعض المظاهر العدولية عند كل من سيبويه والجرجاني ليست من باب التكرار، وإنما من باب أنّ بعض المظاهر تناولها سيبويه والبعض الآخر تناولها الجرجاني، هذا من جهة، ومن جهة أخرى لإثبات تنبُّه علماء العربية لمختلف المقاصد التداولية، وإن لم يعبّروا عنها بمصطلحات واحدة كما يظهر عند	تناول كلا من سبويه والجرجاني المظاهر العدولية ودرسنا كلاهما نظرا لتناول الجرجاني مظاهر وسبويه مظاهر أخرى لإثبات تنبه علماء العربية لمختلف المقاصد التداولية وإن لم يعبرو عنها بمصطلحات واحدة كما يظهر عند سيبوية والجرجاني ص65

	سيبويه والجرجاني ص 173	
تفكيك وإعادة تركيب	- المقاربة بالكفاءة نظام جديد وبديل في المنظومة التربوية. ص:6	المنظومة التربوية طبقت نظام جديد يعتمد على المقاربة بالكفاءات ص:ج
سرقة النقاط البحثية	**الفصـــــل الثـــــانـــي** **I. كيفية تصحيح الإملاء** **تصحيح الإملاء** **طريقة تقوية الطلبة في الإملاء** **الأخطاء الإملائية الشائعة** **II. أمثلة تفصيلية عن الإملاء** **اللام الشمسية والقمرية (تدريبات)** **الهمزة (تدريبات)** **هاء التأنيث وتاؤه (تدريبات)**	**الفصـــــل الثـــــانـــي** **1- كيفية تصحيح الإملاء** **تصحيح الإملاء** **طريقة تقوية الطلبة في الإملاء** **الأخطاء الإملائية الشائعة** **2- أمثلة تفصيلية عن الإملاء** **اللام الشمسية والقمرية (تدريبات)** **الهمزة (تدريبات)** **هاء التأنيث وتاؤه (تدريبات)**
سرقة النقاط البحثية	بنية البحث: تتشكل بنية بحثنا من ثلاثة فصول وكل فصل يحتوي على عدة مباحث مصدرة بمقدمة ومدخل، متبوعة بخاتمة. ففي **المقدمة** قمنا باستعراض موجز للتدريس، لغة واصطلاحا، وحددنا من خلالها موضوع بحثنا الذي اخترنا له تدريس قواعد اللغة في الطور المتوسط، وبعد أن بينا أسباب اختيارنا لهذا الموضوع، أثرنا أن نبدأ رحلة التفكير والتدبير في المدخل أو التمهيد العام، انطلاقا من خصائص أركان العملية	تتشكل بينية بحثنا من ثلاثة فصول وكل فصل يحتوي على عدة مباحث مصدرة بمقدمة ومدخل، متبوعة بخاتمة. ففي **المقدمة** قمنا باستعراض موجز للتدريس، لغة واصطلاحا، وحددنا من خلالها موضوع بحثنا الذي اخترنا له تدريس قواعد اللغة في الطور المتوسط، وبعد أن بينا أسباب اختيارنا لهذا الموضوع، ثرنا أن نبدأ رحلة التفكير والتدبير في المدخل أو التمهيد العام، انطلاقا من خصائص أركان لعملية

	التعليمية (المدرس، المتعلم، المنهج)، وتعريف للنحو والصرف، وتقتضي بنا نهاية هده الرحلة الأولى إلى تحديد واضح للتدريس قواعد اللغة . بحيث تسمح لنا أن نتتبع بارتياح كل المباحث التي تضمنتها فصول هذا البحث، ولذلك نبدأ رحلة هذا البحث بثلاثة فصول متضمنة عدة مباحث. الفصل الأول تحت عنوان طبيعتها ووظيفتها ويحتوي على ثلاثة مباحث، الأول تحدثنا فيه على طبيعة اللغة ووظيفتها، والثاني تناولنا فيه أهداف اللغة والنظريات النفسية التي تحكم تعلم هذه اللغة، والثالث الطرائق الشائعة في تدريس اللغة والتعقيب عليها. الفصل الثاني تحت عنوان قواعد اللغة وطرق تدريسها (نحوا وصرفا)، يحتوي على مبحثين، المبحث الأول تناولنا فيه طرق تدريس قواعد اللغة في الطور المتوسط وأهداف تدريسها، والثاني تحدثنا فيه على صعوبة تدريس هذه القواعد والأساليب الحديثة في تدريس القواعد وتجاوز تلك الصعوبات.	التعليمية (المدرس، المتعلم، المنهج)، وتعريف للنحو والصرف، وتقتضي بنا نهاية هده الرحلة الأولى إلى تحديد واضح للتدريس قواعد اللغة . بحيث تسمح لنا أن نتتبع بارتياح كل المباحث التي تضمنتها فصول هذا البحث، ولذلك نبدأ رحلة هذا البحث بثلاثة فصول متضمنة عدة مباحث. الفصل الأول تحت عنوان طبيعتها ووظيفتها ويحتوي على ثلاثة مباحث، الأول تحدثنا فيه على طبيعة اللغة ووظيفتها، والثاني تناولنا فيه أهداف اللغة والنظريات النفسية التي تحكم تعلم هذه اللغة، والثالث الطرائق الشائعة في تدريس اللغة والتعقيب عليها. الفصل الثاني تحت عنوان قواعد اللغة وطرق تدريسها (نحوا وصرفا)، يحتوي على مبحثين، المبحث الأول تناولنا فيه طرق تدريس قواعد اللغة في الطور المتوسط وأهداف تدريسها، والثاني تحدثنا فيه على صعوبة تدريس هذه القواعد والأساليب الحديثة في تدريس القواعد وتجاوز تلك الصعوبات.

	الفصل الثالث هو الجانب التطبيقي وفيه مبحث واحد، قدمنا فيه دروس نموذجية لطرق تدريس النحو والصرف في الطور المتوسط. وبعد ذلك تأتي الخاتمة التي نجمل فيها ما نعالجه وما نناقشه من قضايا، وما ننتهي إليه من نتائج عامة. ص:ــ ه ــ	الفصل الثالث هو الجانب التطبيقي وفيه مبحث واحد، قدمنا فيه دروس نموذجية لطرق تدريس النحو والصرف في الطور المتوسط. وبعد ذلك تأتي الخاتمة التي نجمل فيها ما نعالجه وما نناقشه من قضايا، وما ننتهي إليه من نتائج عامة. ص:ج ــ
فقرات محشورة	فالكتابة السليمة هي دليل على أن الفاعل متمكن من القواعد الإملائية والنحوية والصرفية واللغوية، فكل هذه القواعد هي كل متكامل وطريق لوجهة واحدة.	كما جرت العادة فإن كل بحث يجب أن ينتهي بخاتمة شاملة وجامعة لكل ما تناوله هذا الأخير – البحث – إذ نجد أن المقاربة بالكفاءة هي بيداغوجيا نفعية معرفية، لذا من الضروري بذل الجهد الكافي لتحقيق هذه المقاربة في مختلف المواد الدراسية، ونحن اخترنا مهارة الإملاء في ظل هذا النظام الجديد لنوصل فكرة أن الإملاء وقواعدها مهمة. فالكتابة السليمة هي دليل على أن الفاعل متمكن من القواعد الإملائية والنحوية والصرفية واللغوية، فكل هذه القواعد هي كل متكامل وطريق لوجهة واحدة. ومن خلال ما أخذناه وما تناولناه في بحثنا هذا توصلنا إلى جملة من أهم النتائج نلخصها فيما يلي:

جدول يبين نسبة أنواع السرقة في مذكرة ليسانس 01: عدد الفقرات النص الإجمالي: 2123:

طريقة حساب الجدول عدد التكرارات قسمة عدد الفقرات ونضرب 100

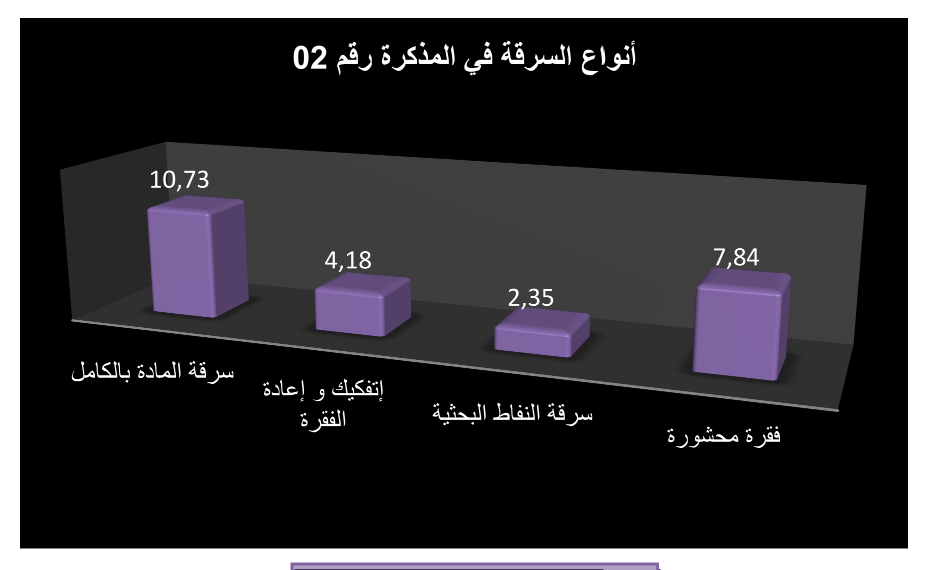
أنواع السرقة	التكرار	النسبة المئوية
سرقة المادة بالكامل	175	**8.24**
تفكيك وإعادة تركيب	**65**	3.06
سرقة النقاط البحثية	**30**	1.41
فقرات محشورة	**122**	5.74
مجموع	392	18.36



شكل رقم :03

جدول يبين نسبة أنواع السرقة في مذكرة ليسانس 02: عدد الفقرات النص الإجمالي: 2078

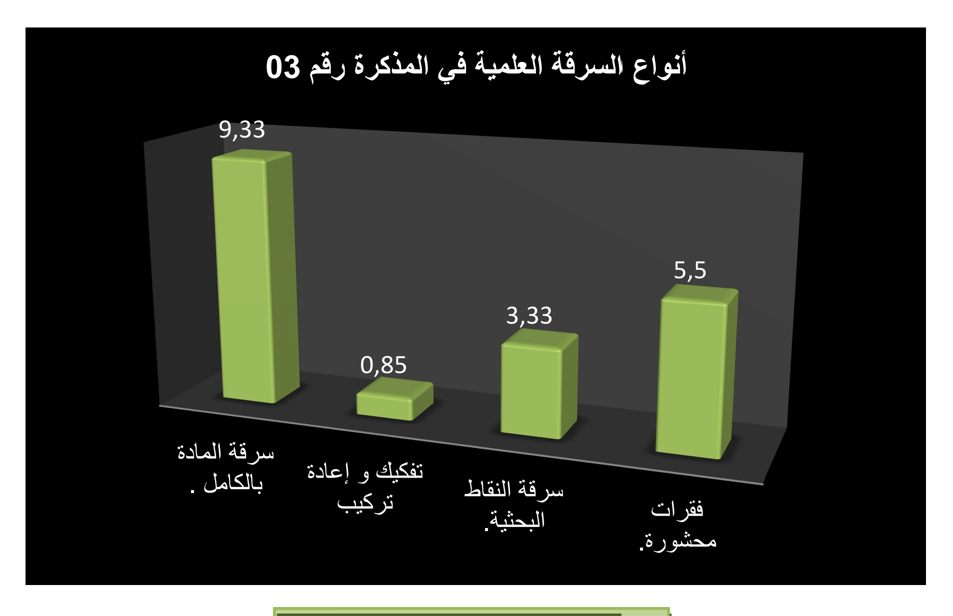
أنواع السرقة	التكرار	النسبة المئوية
سرقة المادة بالكامل	223	**10.73**
تفكيك وإعادة تركيب	**87**	4.18
سرقة النقاط البحثية	**49**	2.35
فقرات محشورة	**163**	7.84
مجموع	392	25.10



شكل رقم :04

جدول يبين نسبة أنواع السرقة في مذكرة ليسانس 03: عدد فقرات النص الإجمالي : 1746

أنواع السرقة	التكرار	النسبة المئوية
سرقة المادة بالكامل	163	**9.33**
تفكيك وإعادة تركيب	**15**	0.85
سرقة النقاط البحثية	**67**	3.33
فقرات محشورة	**97**	5.55
مجموع	392	19.06



شكل رقم :05

تحليل الجداول:

من خلال نتائج إحصاء الجداول التي تبين نسبة أنواع السرقات العلمية من المذكرات رقم: 01-02-03. نقوم بتحليل النتائج ودراساتها وتصنيفها، حيث أحصينا أنواع السرقة العلمية الشائعة والمتكررة للمذكرات معتمدين على نسبة ذيوع نوع السرقة في محتوى المذكرات، حيث تمثل نسبة (8.24) بالمائة في المذكرة رقم: 01 وفي المذكرة رقم: 02 وجدنا نسبة (10.73) وكذلك في المذكرة رقم: 03 وجدنا (9.33) سرقة المادة بالكامل ونالت الحصة الأسد من كل أنواع السرقات ويعود هذا إلى سهولة طريقة السرقة. والعجز والتكاسل العلمي: فمنهم من لا يملك ملكة البحث العلمي، ولا يقوى على خوض غماره، وسبر أغواره، بل لا يقوى على ذلك، مما يدعوه إلى التكاسل عن الكتابة، ويجدون أن كتابة غيرهم أسهل وأسرع.

كما مثلت نسبة (3.06) في الذكرة رقم:1 ونسبة (4.18) في المذكرة: 2 ونسبة (0.85) في المذكرة رقم: 03 من سرقة النقاط البحثية ونرجعه إلى غياب الثقافة المتعلقة بالملكية الفكرية لدى طلبة الليسانس والذي همه الوحيد إنهاء مذكرة لهضم منهجية البحث لا غير، دون إبداع وتفكير في خطط بحثية جديدة وهذا يدخلهم في الركود الإبداعي.

أما بالنسبة لسرقة الفقرات المحشورة فوجدنا النسب الثلاث على المذكرات الثلاث بالتوالي '(1.41)، (2.35) (5.55) ونفسر هاته النسب بجهل الطلبة فهم يتورطون في مشكلة عدم التفريق بين ما يمكن استخدامه بدون توثيق وما لا يجوز، فهم يبدؤون الصفحة بأفكارهم وسرعان ما يحشرون فقرات من الرسالة المحملة من الشبكة العنكبوتية.

ولاحظنا أن الطالب غير قادر على تفكيك وتحليل وإعادة تركيب الجمل والفقرات يرجع إلى ضيق الوقت وفقدانه ملكة التحليل وصياغة الأفكار بأسلوب

جديد نظرا لمحدودية رصيده المعلوماتي ولهذا قدرت نسبته في المذكرة:01 (5.74) وفي المذكرة رقم: 02 (7.84) وفي المذكرة رقم:03 (5.55).

خاتمة: بعد ما قمنا به في هذه الدراسة من حيث الجانب النظري والجانب التطبيقي توصلنا إلى النتائج التي تكشف عن واقع الجريمة الإلكترونية لطلبة السنة الليسانس والتي توصلنا إليها بصعوبة من جهة نقص المصادر والمراجع في هذا الموضوع ومن جهة أخرى ابتكرنا طريقة جديدة تشبه برامج الكمبيوتر في عد وكشف أنواع السرقة يدويا ويمكن بلورة هاته النتائج فيما يلي:

- **إلى أن الاجرام المعلوماتي متعدد ومختلف**
- **بقاء سرقة المعلومة أخطر الجرائم الغير مضبوطة إلى اليوم خاصة أن منطلقها العالم الافتراضي**
- السرقة العلمية هي جريمة معلوماتية تعززت بعض تطور شبكات الإنترنت وانتشارها
- لا يوجد فهم لدى الطلبة حول الجريمة الالكترونية أو السرقة العلمية
- عدم التوصل إلى مفهوم عام متفق عليه حول الجريمة الإلكترونية والنشاط الإجرامي الإلكتروني.
- السمة المميزة للكثير من الجرائم المعلوماتية هي أنها من النوع العابر للحدود، ولهذا يجب إبرام معاهدات بين الدول.
- تدني المهارات البحثية اللغوية لطلبة الليسانس.
- عدم معرفة الكيفية المثلى للاقتباس والتوثيق.

وانطلاقا من تحليل النتائج نتوصل إلى مجموعة من التوصيات:

- الاهتمام بالتربية وتنشئة أفراد المجتمع تنشئة سليمة صحيحة، وتعريفهم بعواقب ما يرتكب من جرائم إلكترونية في الدنيا والآخر.
- الاهتمام بدور مؤسسات المجتمع بدءا من الأسرة والمؤسسات التعليمية وانتهاء بالمساجد والأندية في توعية أفراد المجتمع، بالجرائم، والسرقة الإلكترونية.

- التعاون بين البلدان العربية والدولية لمحاربة الجريمة الإلكترونية. وتفعيل الاتفاقيات التي تكفل مكافحتها والحد من استفحالها- .
- تطوير نظم وأجهزة العدالة والقضاء، ودعمها بخبراء من ذوي الاختصاص في الحواسيب والشبكات. للمساعدة في تكييفها -ضرورة التعاون والتفاهم بين أجهزة العدالة والمؤسسات المالية والبنوك وإلزامها بالإبلاغ عما يحدث لديها من اختراقات إلكترونية، وعدم التستر عليها؛ للمساهمة في مكافحتها.
- تطوير احصائيات دورية لظاهرة الجربمة الالكترونية، وإنشاء قاعدة بيانات بالجرائم التي جرى ضبطها وإصدار عقوبات بشأنها.
- تشديد العقوبات الرادعة بحق الجناة في السرقة الإلكترونية، وإقامة الحد الشرعي إن توافرت شروط إقامته دونما شبهات، فلم يشرع الحد إلا لمحاربة الجريمة، وقطع دابر الفساد والإفساد.
- إجراء المزيد من البحوث والدراسات المقارنة في مجال الجرائم والسرقة الإلكترونية؛ لأنه مجال مستحدث ويتطور باستمرار، ولما يأخذ ما يكفي من الدراسات لاسيما في العقوبة.
-

قائمة المصادر والمراجع:

1- عمرو خالد زريقات: عقد البيع عبر الانترنت دراسة تحليلية. ط 1.د ت. ص: 11.

2- حسن قاسم محمـــد، التعاقد عن بعد جامعة الاسكندرية ط 5، د ت، د ن. ص 13.

3- ويكيبيديا الموسوعة الحرة http://ar.wikipedia.org/wiki

4- منذر محمد الجنيبهي: الطبيعة القانونية للعقد الإلكتروني دار الفكر الجامعي، دط الاسكندرية، بدون سنة النشر، ص :07.

5- عمر خالد زريقات عقد البيع عبر الأنترنت دراسة تحليلية الطبعة الأولى دون نشر، ص :20.

6- ناجي الزهراء: التجربة التشريعية في تنظيم المعاملات الإلكترونية المدنية والتجارية، جامعة بومرداس، الجزائر، 2009 -2010، ص:02.

7- نذير برني: العقد الإلكتروني على القانون المدني الجزائري مذكرة لنيل إجازة المدرسة العليا للقضاء، دفعة 2003-2006، ص: 32.

8- أساس الجريمة المعلوماتية هي العولمة والتصرفات المجرمة قانونا التي يمكن أن تقع عليها أو بواسطتها والتي قد تمس بمال غير أو بالأشخاص والحريات.

9- سامي علي حامد عياذ، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الاسكندرية 2007، ص 40 -39-38.

10- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في الجرائم الكمبيوتر والأنترنت دار الكتب القانونية مصر 200، ص 1.

11- خالد ممدوح إبراهيم، الجريمة الإلكترونية، الدار الجامعية، الإسكندرية 2008، ص 4.

12- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة للنشر، ط 2001 الإسكندرية، ص 61، 62.

13-خالد ممدوح ابراهيم / أمن الجريمة الإلكترونية، الدار الجامعية الإسكندرية، 2008، ص 49، 50، 51.

14-12- محمد علي العريان، الجرائـم المعلوماتيـة، دار الجامعـة للنشر ط 2001، الإسكندرية، ص 74.

15- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في الجرائم الكمبيوتر والأنترنت دار الكتب القانونية مصر 200، ص 6.

16- خالد ممدوح إبراهيم، الجريمة الإلكترونية، الدار الجامعية، الإسكندرية 2008، ص 15 -http://www.library.qu.edu.sa/Res_Gui_prog/Pages.

16 -https://ijnet.org/ar/blog/134312.

17 -http://www.vetogate.com/1701019

18 -http://www.vetogate.com/1701019.

العلاقة التأثيرية بين الأمن المعلوماتي والأمن القومي للدول: بين متطلبات التطور والتكامل ورهانات التهديدات

شاطري كاهنة.

جامعة مولود معمري، تيزي- وزو

ملخّص: يعتبر الأمن مطلب غريزي وأساسي في حياة المجتمعات والأفراد وهدف أسمى للدول في سياستهم الداخلية والخارجية، مثلما يلعب دورا مهما في تحديد طبيعة العلاقات الدولية من صراع أو تعاون، فهو يدخل في مختلف عمليات التنمية الشاملة للدول: سياسيا، اقتصاديا، اجتماعيا، ثقافيا...الخ، وبذلك يحتل الأمن مكانة بارزة في ذهنيات واستراتيجيات صناع القرار للدول.

وبدخول العالم عصر المعلوماتية بفعل الثورة التكنولوجية والمعلوماتية وتلاشي الحواجز بين الشعوب والدول، ظهر بعد آخر للأمن القومي، وهو "الأمن المعلوماتي"، على إثر إقحام المعلوماتية في جميع التفاعلات للدول، وظهور أيضا ما يعرف بـــ "الحوكمة الإلكترونية"، الواقع الذي وضع الدول أمام أخطار وتحديات استلزمت استحداث نظم وبرامج لحماية الشبكات والمواقع الالكترونية.

مقدّمة: يعرف العالم اليوم مرحلة جديدة من التطور التكنولوجي بفعل "**الثورة المعلوماتية**" التي أفرزتها العولمة إذ تطورت التقنيات المعلوماتية، التي جاءت نتيجة للتدفق السريع للمعلومات، وتضاعف الإنتاج المعرفي في جميع القطاعات الحيوية للدولة: السياسية، العسكرية، الاقتصادية، الاجتماعية، كما أدّت إلى بروز مصطلحات كـــ: **المجتمع المعلوماتي، الحكومة الالكترونية**، حيث انتقلت الحكومة من شكلها التقليدي إلى الحكومة الالكترونية أين أصبحت صفة "**الإلكترونية**" ملتصقة بجميع المجالات والتخصصات، وعليه أصبحت قوة الدول تقاس نسبة إلى

مدى امتلاكها أو افتقارها للتقنيات المعلوماتية، التي أصبحت أبرز مظاهر القوة المعاصرة.

ومواكبة لهذا الكم الهائل من المعلومات التي يعرفها عالم المعلوماتية والشبكات الالكترونية الموسعة أصبح الحديث عن "**الأمن المعلوماتي**"، الذي يستوجب استحداث نظم معلوماتية متطورة وعالية المستوى، على إثر الآثار السلبيات التي خلفتها "الثورة المعلوماتية"، بالرغم من كل ايجابياتها في اختصار الوقت والمال والجهد فتطوّر التقنيات المعلوماتية الكبير، زاد من قابلية التعرض للتهديدات الالكترونية المتمثلة في "**الجرائم المعلوماتية**" لذلك ساهمت البيئة الرقمية المفتوحة في بروز تهديدات جديدة وخطيرة على الأمن القومي للدول، من خلال تعريض البنى التحتية للدولة للانكشاف المعلوماتي، وانتقلنا للحديث عن صراعات رقمية وحروب رقمية، وإرهاب الكتروني، على خلفية البعد العابر للحدود للمعلوماتية.

لذا كان لزاما على الدول صياغة الاستراتيجيات التدابير الأمنية المعلوماتية الكفيلة لحماية البيانات الرقمية، كما أنّ الأمن المعلوماتي أصبح بعدا وعنصرا حيويا لحماية الأمن القومي للدول، لكن الافتقار إلى المهارات المعلوماتية المتعلقة بالبنى التحتية للدول النامية والعربية، أضحى تحديا كبيرا أمام تطبيق السياسات الأمنية القومية الناجعة.

أهمية المداخلة: تبرز أهمية الموضوع في كون أنّ المعلومات أصبحت تدخل في جميع التفاعلات بين الدول بكل أنواعها وأنّه وبالرغم من ايجابيات الثورة المعلوماتية، إلا أنّ السلبيات فرضت نفسها على واقع الأمن القومي للدول بالتالي محاولة تبيان مهددات الأمن المعلوماتي على الأمن القومي، وطبيعة العلاقة التأثيرية بينهما.

هدف المداخلة: يهدف الموضوع إلى تبيان المفاهيم المختلفة للأمن بالنسبة للدول، وأثر التحولات الدولية على إحداث تغيرات على مستوى مصادر تهديد القومي وانعكاساتها عليه، وإلقاء الضوء على تهديدات "الأمن المعلوماتي" وأثرها

على الأمن القومي للدول، مع محاولة إبراز الاستراتيجيات والتدابير الأمنية الكفيلة لتحقيق علاقة تكاملية بين الأمن المعلوماتي والأمن القومي.

منهج المداخلة: اعتمدنا على المنهج الوصفي التحليلي، من خلال دراسة وتحليل أهمية وآليات تحقيق الأمن سواء بالنسبة للأمن القومي أو بالنسبة للأمن المعلوماتي، مع التطرق إلى أهم الاستراتيجيات والتدابير الأمنية المعلوماتية والقومية الازمة لتحقيق علاقة تكاملية بين الأمن المعلوماتي والأمن القومي.

وبناءً على ما تقدم نطرح الإشكالية:

كيف أثرت الثورة المعلوماتية والتكنولوجية على واقع الأمن القومي للدول؟ وماهي الاستراتيجيات الكفيلة لتجسيد الأمن المعلوماتي ليحقق علاقة تكاملية مع الأمن القومي في ظل التهديدات الالكترونية الراهنة؟

وتتفرع عن هذه الإشكالية التساؤلات الفرعية التالية:

- فيما يتمثّل مفهوم الأمن والأمن القومي؟ وماذا نعني بالتهديد؟
- فيما تتجلى الثورة المعلوماتية؟
- ماذا نعني بالأمن المعلوماتي؟ وماهي أثر تهديداته على الأمن القومي للدّول؟
- ماهي أهم الاستراتيجيات المعلوماتية والجهود الدولية لحماية الأمن المعلوماتي والأمن القومي معاً؟

وللإجابة على الإشكالية نصيغ الفرضية التالية:

كلما تم استحداث نظم وبرامج ومراكز معلوماتية لحماية الحدود الإلكترونية للدول، تحقق البعد التكاملي في العلاقة التأثيرية بين الأمن المعلوماتي والأمن القومي.

وسنحاول معالجة الإشكالية وفقا للمحاور التالية:

- **المحور الأول:** مفهوم الأمن.
- **المحور الثاني:** مفهوم الأمن القومي والمقاربة النّظرية للأمن في العلاقات الدّولية.

- **المحور الثالث:** مفهوم الثورة المعلوماتية.
- **المحور الرابع:** مفهوم الأمن المعلوماتي.
- **المحور الخامس:** مهدّدات الأمن المعلوماتي وأثرها على الأمن القومي.
- **المحور السادس:** استراتيجيا حماية الأمن المعلوماتي والجهود الدولية للحد من المخاطر المعلوماتية.
- **خاتمة:** النتائج والتوصيات

المحور الأوّل: الأمن: المفهوم والمستويات

يعتبر الأمن من المفاهيم الأساسية في العلوم الإنسانية عموما، والعلاقات الدولية خصوصا، لذلك ارتأينا تناول أهم التعاريف التي تجاذبته، ومختلف مستوياته.

أولا: مفهوم الأمن

يحتل موضوع الأمن أهمية كبرى في الدراسات الدولية باعتباره يشكل محور بحث أساسي في كتابات واهتمامات دارسي العلاقات الدولية، ويمكن حصر هذه الأهمية في مستويين[1]:

1- **المستوى الأكاديمي**: تتجلى هذه الأهمية من خلال مركزية موضوع الأمن كبرنامج بحثي في الأطر والمقتربات النظرية الكلاسيكية والمعاصرة للعلاقات الدولية، فالأمن هو إحدى تركيبات وعمليات السياسة العالمية.

2- **المستوى التطبيقي**: تتجلى هذه الأهمية من خلال مدى إدراك الدول لبيئتها الأمنية داخليا وخارجيا وانعكاس ذلك على صياغة منظوماتها الأمنية بشكل توافقي أو تعارضي، استنادا إلى مقوماتها وإمكاناتها الداخلية وارتباطا بتموقعها في النظام الدولي.

يرى "**أرنولد ولفرز Arnold Welfers**" أنّ الأمن في جانبه الموضوعي يعني: "**غياب أيّة تهديدات اتجاه قيم مكتسبة، وفي جانبه الذاتي فهو يعني غياب الخوف من أن يتم المساس بأية من هذه القيم**"[2].

ويعرّف "**باري بوزان Barry Buzan**" الأمن على أنّه: "**وجود درجات عالية من التماسك الاجتماعي، وانخفاض مستويات العنف السياسي الداخلي**"[3].

ويعرف "**زكريا حسين**"* الأمن على أنّه: "القدرة التي تتمكن بها الدولة من تأمين انطلاق مصادر قوتها الداخلية والخارجية، الاقتصادية والعسكرية في شتى المجالات في مواجهة المصادر التي تتهددها في الداخل والخارج، في السلم والحرب، مع استمرار الانطلاق المؤمَّن لتلك القوى في الحاضر والمستقبل تخطيطاً للأهداف المخططة"[4].

عموما، يرتبط مفهوم الأمن بأربع دلالات، وهي[5]:

أ- **من الناحية النفسية:** الأمن هو اختصار التحرر من شعور الانعدام الأمني كبديل لاحتمالية التهديد الأمني.

ب- **من الناحية السياسية:** الأمن يشير إلى سلامة أراضي الدولة واستقلالها السياسي، وحمايتها من التهديدات في الداخل أو من الخارج لإيجاد الظروف الملائمة لكي تتمكن الدولة من تحقيق مصلحتها الوطنية.

ت- **من الناحية التنموية:** هناك علاقة تناسب طردي بين الأمن والتنمية ويعتبر "**روبرت ماكنمارا Robert Macnamara**" أحد رواد هذا الطرح، إذ يقول: "إنّ الأمن ليس هو المعدات العسكرية وإن كان يتضمنها، والأمن ليس هو النشاط العسكري وإن كان يشمله، إنّ الأمن يعني التنمية وبدون التنمية لا يمكن أن يكون هناك أمن، فإذا لم توجد هناك تنمية داخلية أو على الأقل درجة أدنى منها فإنّ النّظام والاستقرار يصبحان أمرا صعبا".

ث- **من الناحية الاجتماعية:** يرى "**جون غالتونغ John Galtung**" في دراسته "**الأشكال البديلة للدفاع Les Formes Alternatives de defense**" كيف أنّ البناء الأمني للدول لم يعد معزولا عن تأثيرات البيئة الاجتماعية التي تؤثر على الأمن القومي، بإيجادها حالة من اللاتعاون أو التمرد الجماعي العام، وتتلخص الدلالة الاجتماعية للأمن في فكرة مفادها أنّ للأمن القومي جوانب اجتماعية تعكس

العلاقة الوطيدة بينهما، وهذا ما يتطلب من الدولة تعبئة القوى الاجتماعية باختلاف مراكزها في المجتمع من أجل المشاركة في مواجهة جماعية لتحديات الأمن القومي نتيجة تعقيدات الحياة المعاصرة.

ثانيا: مستويات الأمن:

للأمن أربعة مستويات، وهي[6]:

- **الأمن الفردي:** أمن الفرد ضد أية أخطار تهدد حياته أو ممتلكاته أو أسرته.
- **الأمن القومي (الوطني):** ويعني حماية الوطن ضد أية أخطار خارجية أو داخلية للدولة.
- **الأمن القُطري أو الجماعي:** ويعني اتفاق عدة دول في إطار إقليم واحد على التخطيط لمواجهة التهديدات التي تواجهها داخليًّا وخارجيًّا، وهو ما يعبر عنه "**بالأمن الإقليمي**".
- **الأمن الدولي:** وهو الذي تتولاه المنظمات الدولية سواء منها الجمعية العامة للأمم المتحدة أو مجلس الأمن الدولي ودورهما في الحفاظ على الأمن والسلم الدوليين.

وسنحاول التركيز في بحثنا على المستوى الثاني المتعلق بالأمن القومي.

المحور الثاني: مفهوم الأمن القومي والمقاربة النظرية للأمن والتهديد في العلاقات الدولية

إنّ تحقيق الأمن القومي هو هدف كل السياسات العليا والدنيا للدول، وتتزايد أهمية هذا المفهوم بالنظر لتطور المقاربة النظرية لتفسير ظاهرة الأمن والتّهديد في العلاقات الدولية.

أولا: مفهوم الأمن القومي

يحظى الأمن القومي باهتمام جميع المراكز البحثية في العلاقات الدولية باعتباره النواة الأساسية لاستقرار الفرد بالدرجة الأولى، والنظام ككل بالدرجة الثانية، إذ كان تحقيق الأمن القومي أساس كل السياسات التي تنتهجها الدول ومنها

الاستعمارية، وركيزة أساسية للقرارات الاستراتيجية التي يتخذها القادة، وأهمها: خوض الحروب، وعليه وجب علينا تحيد مفهوم الأمن القومي، علما أنّ هذا المصطلح ظهر نتيجة قيام الدولة القومية في القرن السادس عشر ميلادي، بعد توقيع معاهدة واستفاليا عام 1948م، ليُعبّر فيما بعد عن الأمن القومي بمصطلحات أخرى، مثل: المصلحة القومية، سيادة الدّولة والإرادة الوطنية.

فالأمن القومي: عبارة عن الحالة التي تصل إليها الدولة، بحيث تكون قيم الدولة العليا من: ثقافة الدولة ومبادئها ووحدتها ورفاهية الأفراد بها، محفوظة وفي تطور مستمر[7].

وينقسم تعريف الأمن القومي إلى جزأين[8]:

- **الأمن القومي الداخلي:** وهو الأمن الذي بموجبه يتم الحفاظ على استقرار الحدود الداخلية للبلاد، بما يتضمّن ذلك الحفاظ على الحدود الجغرافية والحفاظ على المنشآت العامة، وتختلف المصطلحات التي تتدرج تحت تعريف الأمن القومي الداخلي تبعا لحجم الدّولة وظروفها الاجتماعية والاقتصادية وموقعها الجغرافي وعموما يشمل الأمن القومي الداخلي: القدرة العسكرية، الاستقرار السياسي الاقتصادي والاجتماعي.

- **الأمن القومي الخارجي:** يتعلق الأمن القومي الخارجي بحماية الدولة من الأخطار الخارجية المتعلقة بدول الجوار أو الدول المتربصة بسلامة الدولة، وتوجد العديد من الأدوات للحفاظ على الأمن الخارجي للبلاد، أهمها: الأدوات الدبلوماسية.

ثانيا: المقاربة النظرية للأمن والتهديد في العلاقات الدولية

باعتبار أنّ مفهوم الأمن مفهوم محوري في العلاقات الدولية، فقد تناولته العديد من النظريات، كمحاولات تفسيرية للواقع الدولي، خاصة في ظل اختلاف مصادر التهديد من مرحلة إلى أخرى، وتنامي أشكالها.

لقد كان المفهوم التقليدي للأمن والذي تبنته النظرية الواقعية يُعنى فقط بالدّولة وحماية حدودها الجغرافية، بحيث كانت الفاعل الرئيسي وكمستوى تحليل وحيد في

العلاقات الدولية، فالنظرة التقليدية للأمن تقوم على أنّ الوظيفة الأساسية لأيّ نظام سياسي –الدّولة– البقاء والاستمرار الذي لا يتم إلا عن طريق القوة العسكرية وتعتبر المقاربة الواقعية التقليدية للأمن الإطار النظري والمرجعي للدراسات الاستراتيجية والسياسات الأمنية بعد الحرب العالمية الثانية وفترة الحرب الباردة إلا أنّه بداية السبعينات ظهرت متغيرات وفواعل جديدة في العلاقات الدولية كالعولمة، التهديدات غير العسكرية وظهور الشبكات الإرهابية، هذا ما أدى إلى ظهور قراءة جديدة للواقع الدّولي[9].

وفي ظل هذه التحولات برز التشكيك في صلاحية النظرية الواقعية (النظريات التفسيرية أو الوضعية) في تفسير واقع ما بعد الحرب الباردة بعد زوال الخطر السوفياتي، وبرزت اتجاهات تطالب إعادة النظر في مفهوم الأمن ليواكب الواقع الدولي الجديد، الأمر الذي تدعّم من خلال تقرير "إيجون بار Egon Bahr" المقدم للجنة Palme (1982)، تحت عنوان "الأمن المشترك"، للتصدي لما يعرف بـــ "المأزق الأمني" في ظل بروز أشكال أخرى من المخاطر التي تتهدد الدول، الأمر الذي أدى على تبني مفهوم أوسع للأمن بمسميات متعددة، وهي[10]:

- **الأمن المتكامل Comprehensive Security**: ويتضمن كل أشكال التهديد.
- **الشراكة الأمنية Security Partnership**: يتم إشراك الدول غير الغربية.
- **الأمن المتبادل Mutual Security**: إذ يتم التخلي نسبيا عن نزوع الدول منفردة إلى تعظيم أمنها على حساب الدّول الأخرى.
- **الأمن التعاوني Cooperative security**: بحيث يتم تقاسم الأعباء الأمنية لاحتواء التهديدات.

ولعل من الإسهامات النظرية المهمة التي ظهرت في حقل الدراسات الأمنية تلك التي تبنتها "مدرسة كوبنهاغن"، إذ تولّ عدد من الباحثين مهمة إخراج الأمن من المفهوم الضيق إلى المفهوم الموسع، وعلى رأسهم: "**باري بوزان Barry**

"**Buzan**" و"**أول وايفر Ole Woever**"، بحيث أصبح يشمل الأمن خمسة قطاعات أساسية، وهي[11]:

- **الأمن العسكري:** ويشمل القدرات العسكرية الدفاعية والهجومية للدّول.
- **الأمن السياسي:** استقرار مؤسسات النظام السياسي.
- **الأمن الاقتصادي:** قدرة الدولة على بلوغ الموارد المختلفة والإمكانات المالية اللازمة.
- **الأمن المجتمعي:** الاستقرار الثقافي والهوياتي، إشارة المجموعة لنفسها بضمير "**نحن**".
- **الأمن البيئي:** حماية البيئة من الممارسات الانسانية التي ينتج عنها ظواهر كـــ : تغير المناخ، الاحتباس الحراري، التلوث، الجفاف...إلخ.

أمّا أصحاب المدرسة النقدية وعلى رأسها "**ماكس هوركايمر Max Horkheimer**"، فاعتبروا أنّ الفرد هو المرجعية الأساسية في الدارسات الأمنية فالأمن يعني: غياب التهديدات والتحرر من الاكراهات المادية والانسانية التي تمنع الأفراد من القيام باختياراتهم.

فيما يخص مفهوم "**التهديد**" في العلاقات الدولية بمفهومه الاستراتيجي: هو بلوغ تعارض المصالح والغايات القومية مرحلة يتعذر معها إيجاد حل سلمي يوفّر للدول الحد الأدنى من أمنها السياسي والاقتصادي والاجتماعي والعسكري[12].

ويمكن تحديد أهم ملامح الظاهرة الأمنية في الواقع المعاصر على النحو التالي[13]:

- الظاهرة الأمنية المتعدية لحدود الدولة القومية .
- اتساع نطاق مصادر التهديد.
- تعدد نوعية مصادر التهديد الأمني.
- ظهور نوعية جديدة من التهديدات الأمنية التي لم تكن معروفة من قبل.
- تغير مضمون التهديدات الأمنية التقليدية، وتغير الوزن النسبي لأهميتها.

لذلك وجب علينا الإحاطة بمجموعة من العوامل التي تؤثر في تحديد التهديدات التي تواجه الأمن، ونذكر منها[14]:

– **طبيعة التهديد:** ويُقصد به نوعه وأبعاده، سواء السياسية أو الاقتصادية أو العسكرية أو الجغرافية.

– **مكان التهديد:** اتجاهاته ومدى قربه أو بعده الجغرافي أو الديمغرافي، سواء كان مباشراً أو غير مباشر ومدى انتشاره وتأثيره الشامل لعدة دول، أو محدد في دولة معينة.

– **زمان التهديد:** تأثيره الحالي أو المستقبلي، ومدى استمراريته (مؤقت– مستمر)، وهل هو ثابت أو متغير.

– **درجة التهديد:** قوته وخطورته، حيث كلما زادت درجة قوة التهديد وخطورته تطلّب ذلك تعبئة شاملة للقوة الإقليمية للحد من تأثيره.

– **تعبئة الموارد:** تعبئة الموارد: ترتبط بحجم وخطورة التهديد، ومدى كثافته الأمر الذي يتم في ضوئه اتخاذ إجراءات تعبئة مناسبة من حيث حشد الموارد والجهود للجدّ من تأثيره وأبعاده.

وعليه، فإنّ إدراك التهديدات ينبع من تتبع وفهم حقيقة التحولات المعاصرة الدولية منها والإقليمية، وانعكاساتها على مضامين الأمن ومصادر التهديدات وسبل مواجهتها، وفي ضوء هذه التحولات الدولية برز ما يعرف بـــ "الثورة المعلوماتية" وما صاحبها من آثار على الأمن في إطار إشكالية أمنية ومفهوم أمني جديدين، وهي "الأمن المعلوماتي".

المحور الثالث: مفهوم الثورة المعلوماتية

أصبحت "**الثورة المعلوماتية**" واقعاً ضروريا فرض نفسه في زمن العولمة، إذ ساهمت في إزالة الحواجز القائمة بين الشعوب والدول، وغدت المسارات الإلكترونية تتجاوز الحدود القانونية الدولية القائمة في مختلف دول العالم، ووحدت سبل الاتصال القائمة بين سكان مختلف مدن العالم وبلغاتهم المتعددة، وأضحت

الثورة المعلوماتية واحدة من الأدوات التي تسمح للتطور التاريخي البشري بالخروج من المستويات المعتادة إلى مستويات جديدة وجاء ذلك تحت تأثير تقنيات شبكات الاتصال (**Networking technologies**) الأمريكية التي ارتبطت بها أهم مراحل الثورة المعلوماتية خلال القرن العشرين[15].

وهي ثورة ديناميكية مركبة تشتمل على أربعة تغيرات سريعة أساسية على الأقل[16]:

– القفزة الكبيرة لتكنولوجيا الحوسبة ومعالجة المعلومات واندماجها مع التقدم المذهل لوسائل الاتصال (الهاتف، التلفزيون والمحطات الفضائية) في منظومة تقنية واحدة.

– التطور غير المسبوق في تراكم المعرفة والانتقال من المعرفة العلمية إلى تطبيقاتها العملية (التكنولوجية) بسهولة أكبر في زمن أقل من جهة، والسرعة العجيبة في نقل هذه المعرفة وتعميمها على مستوى العالم نتيجة لذلك الاندماج من جهة ثانية.

– الانترنت (الشبكة الدولية للمعلومات) التي تجمع العالم كله على منابع معلومات حرة، وتتميز الانترنت بأنّ خدمتها تشمل كل الخدمات التي توفرها وسائل الاتصال المختلفة وتتخطاها، وتطرح عددا هائلا من الخيارات، فمع الانترنت بالإمكان الاطلاع على آلاف المواقع التي تعرض جميع أنواع المعلومات وأصنافها الاقتصادية، السياسية، الفنية والبيئية، أي تضع العالم كله بين يدينا.

– وتشمل العواقب والتأثيرات الأكيدة والممكنة والمحتملة التي يتركها ذلك في حياة البشر الاقتصادية والسياسية والثقافية.

وإذا ما حللنا مصطلح "**الثورة المعلوماتية**"، نجد أنّ "***الثورة***" تحمل في طياتها الأمل والحلم الذي واكب الإنسان منذ زمن طويل بالعمل القليل والإنتاج الكثير وتحرره من الأعمال الشاقة، إضافة إلى وجود المعلومات الهائلة بمتناول اليد، مما يدل على حدوث تحسن نوعي على مستوى معيشة الفرد ورفاهيته، وإمكانية

الاتصال مع الآخرين، كذلك بناء ثقافة عالمية وتطويرها، مما يجعل الأرض الواسعة قرية صغيرة بمتناول كل فرد يؤثر فيها ويتأثر بها، وأصبحت تطبق مقولة "من يملك المعلومات يملك القرار"، ممّا قد يطرح العديد من التهديدات على الحريات الأساسية للأفراد[17].

أمّا *"**المعلوماتية**"* ككلمة ترجمة لكلمة مستحدثة تتكون من كلمتين وهما: "**Information**" و"**Automatique**"، وتُعنى بمعالجة المعلومات بطريقة أوتوماتيكية، وبواسطة آلات وأدوات لها قدرة هائلة على القيام بحسابات رياضية واستخلاص نتائج من معطيات أولية.

وتشكل المعلوماتية نقلة كبرى في الوسائل والأساليب التي تنقل المعلومة، وفي سرعة تطور وتراكم المعلومات وتدفقها السريع دون ضوابط، والمعلوماتية مرتبطة "**بالعولمة Globalisation**"، لأنّ المعلومات هي أحد آلياتها، وعليه فالمعلوماتية هي: "**حالة من تسامي قيمة المعلومات وارتفاعها إلى المستوى الذي يجعلها أحدا من عناصر الإنتاج وأحيانا أهمّها، وواحدة من عناصر القوة المعاصرة، وهي حالة تتحقق بفضل التقدم التكنولوجي الهائل في إنتاج المعلومات وإيصالها وتوزيعها**"، لهذا هناك من وصف عصرنا بأنّه: "**عصر اللااستمرارية Discontinuity Age**" [18].

في هذا الإطار، لابد من الإشارة إلى أنّ التطور التقني الذي شهدته الأداة الأولى للمعلوماتية، وهي الآلة، وصل إلى حد أصبح هذا التقدم رهينة للتقدم في المجالين الآخرين، وهما: **البرنامج** الذي أصبح قريبا إلى حد كبير من اللغات والإشارات التي يتعامل بها الأفراد (اللغات الطبيعية)، و**الإنسان** الذي يستعمل ويتعامل مع الآلة والذي يتحتم عليه أن يستوعب ويفهم أهمية الآلة ودورها في علاقاته المختلفة[19].

يعتبر الاستخدام الموسع لشبكات الحاسبات الإلكترونية العالمية بداية منذ عام 1986، أحد أبرز ملامح الثورة المعلوماتية، وتعدّ الولايات المتحدة الأمريكية رائدة

في هذا المجال، وممّا سرع تطور شبكات الاتصال إنشاء منظمات لإدارة الشبكات العابرة للقارات، ففي عام 1989 أحدثت في أوروبا **(RIPE Resaux IP Europeans)** لإدارة وتنسيق عمل الشبكات، ومن أجل تنسيق عمل البنية التحتية العامة، ركزت الجهود لإعداد وإقرار إجراءات تنظيمية تخدم المنظمة، وتضمنت الأجهزة التالية: **الجهاز المركزي (IAB Internet Activities** Board) المؤلّف من لجنتين تابعتين هما: **لجنة الأبحاث (IRTF Internet Research Task Force)**، **واللجنة القانونية (IETF Internet Engineering Task Force)** وتعتبر **IETF الخدمة الإدارية الأساسية للإنترنيت**، وهي تهتم بمسائل المقاييس وتتخذ القرارات في مجالات مقاييس **RFC (Request For Comments)** وتتألف هذه اللجنة التابعة من أقسام متخصصة، وتقسم إلى فرق عمل وفق المهام وكل المقاييس التي أقرتها **IETF** من أجل **RFC** وضعت في متناول الجميع. وبالإضافة إلى ذلك شملت شبكات الإنترنيت منظمة حملت اسم **(NIC Network Information Center)**، تعمل على نشر المعلومات التقنية، وتسجيل وإيصال المستخدمين للشبكات، وإقرار المهام الإدارية مثل: نشر العناوين في الشبكات، أما خدمات الحاسبات الإلكترونية الخاصة للانترنيت في الأقاليم والمنظمات المحلية وبعض الأشخاص، فتقدمها خدمة**(ISP Internet Service Providers)**.[20]

لقد كان نتاج الثورة المعلوماتية ما يسمى بـــ "**المجتمع المعلوماتي**"، الذي أضحت فيه المعلومة الرقمية كأساس مهم في دورة بناء المجتمعات المتقدمة، ومن أبرز عناصر المجتمع المعلوماتي ما يلي:

❖ **<u>الحكومة الالكترونية:</u>** تبلورت تجربة الحكومة الالكترونية في أواسط الثمانينات في الدول الاسكندنافية وتمثلت في ربط القرى البعيدة بالمركز وأطلق عليها اسم "**القرى الالكترونية Electronic villages**" ويعد "**لارس**" من جامعة أدونيس في الدانمارك رائد هذه التجربة، ثم تلتها تجارب في المملكة المتحدة والولايات المتحدة الأمريكية، وتنطلق فكرة "**الحكومة الالكترونية Electronic**

Government" من النّظر إلى المؤسسات والأجهزة الحكومية كمصدر للخدمات والمواطنين، ومؤسسات القطاع الخاص كمستفيدين من هذه الخدمات، وفي عام 2002 عرفت الأمم المتحدة الحكومة الالكترونية على أنّها: "**استخدام الانترنت والشبكة العالمية العريضة لتقديم معلومات وخدمات الحكومة للمواطنين**"، **مثلما عرفتها منظمة التعاون والتنمية في المجال الاقتصادي عام 2003 كالتالي:** "**الحكومة الالكترونية هي استخدام تكنولوجيا المعلومات والاتصالات وخصوصا الانترنت للوصول إلى حكومات أفضل**"[21].

- **<u>التجارة الالكترونية:</u>** وهي العمليات المتمثلة في بيع وشراء وتسويق وتقديم الخدمات الخاصة بالسلع أو الخدمات عبر العديد من شبكات الحاسب الآلي كالانترنت، فقد ساهمت صناعة المعلومات في عصر الثورة التكنولوجية للاتصالات في خلق الوجود الواقعي للتجارة الالكترونية باعتبارها تعتمد بشكل أساسي على الحاسوب وشبكات الاتصال ومختلف الوسائل التقنية بهدف إدارة النشاط الاقتصادي.

- **<u>التعليم الالكتروني:</u>** ويمثّل شكلا من أشكال التعليم عن بعد، ويُعرّف على أنّه: "**طريقة للتعليم باستخدام آليات الاتصال الحديثة كالحاسوب أو الشبكات والوسائط المتعددة**".

- **<u>التوظيف الالكتروني:</u>** وهي خدمة شبكية تسمح باستخدام تكنولوجيا المعلومات والاتصال من قبل المؤسسة لطرح الوظائف الشاغرة المتوفرة لديهم بهدف استقطاب مواهب وكفاءات خارجية لاختيار مرشحين ملائمين، وهذه الخدمة تسهل للأفراد الحصول على فرص عمل، وإعدادهم لتولي مناصب وظيفية تتناسب مع مؤهلاتهم العلمية ما يسمح بتحسين التنافسية والإنتاجية.

- **<u>البيئة الالكترونية:</u>** وتتمثّل في مجمل الخدمات التي توقعها تكنولوجيا المعلومات والاتصالات، بغرض حماية البيئة من الأخطار المحدقة بها وحماية الأفراد والمجتمعات منها.

❖ **<u>الزراعة الالكترونية:</u>** وهي مجال حديث الظهور ضمن العلوم الزراعية ويشير المصطلح إلى تطوير الخدمات الزراعية من خلال دعم وتبادل المعلومات عبر شبكة الانترنت[22].

بالرغم من كل الايجابيات التي أتت بها الثورة المعلوماتية بالنسبة لتسهيل وتسريع نمط الحياة العصرية، إلاّ أنّ ذلك لا ينفي الانعكاسات السلبية التي أفرزتها هذه الثورة، وهذه التقنية العالية، بحيث أدّى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم أصطلح على تسميتها "**الجريمة المعلوماتية**"، بحيث تغيرت أنماط الجريمة، فلم تعد الاعتداءات تستهدف النفس، والمال، واحتلال أراضي فقط بل طالت المعلومات، وهو ما أصبح يعرف على السّاحة الدولية بإجرام ذوي "**الياقات البيضاء**"، إذ تقع الجريمة دون إراقة الدماء ولا التّنقل من مكان إلى آخر وهو ما جعل البعض يصفها بـــ "**الجرائم الناعمة Soft Crime**"، وهذا النّوع من الجرائم ليس مقصورا في دولة أو منطقة معينة، بل مشكلة عالمية[23].

وعلى غرار الجرائم التقليدية، تتميز الجرائم الالكترونية بخصائص منفردة على النّحو التالي[24]:

- الحاسب الآلي هو أداة الجريمة.
- ترتكب هذه الجرائم عبر شبكة الانترنت.
- مرتكب الجريمة هو الإنسان (شخص طبيعي).
- التخصص في الجرائم الالكترونية.
- تعتبر هذه الجريمة عابرة للحدود.

في ظل هذه التهديدات المعلوماتية التي شهدها المجتمع الدّولي بفعل الطفرة التي أحدثتها الثورة المعلوماتية في مجال المعلومات، ظهرت معها مفاهيم أمنية جديدة مواكبة لتلك التحديات الأمنية، تحت عنوان جامع ومانع، وهو: "**الأمن المعلوماتي**".

المحور الرّابع: مفهوم أمن المعلومات: يعد الأمن المعلوماتي من المفاهيم المركزية التي تدخل في تشكيل معظم المنظومات الأمنية المعاصرة، لذا استلزم منا الأمر البحث في جميع المكونات التي تحقق لنا في النهاية مفهوم "أمن المعلومات"

1- **مفهوم المعلومة:** تُعرّف المعلومات على أنّها: البيانات التي تجرى عليها معالجات معينة، وترتيبها وتنظيمها وتحليلها بغرض الاستفادة منها والحصول على نتائج معينة من خلال استخدامها، وهي أداة مهمة وفعالة في التأثير في سلوك الأفراد والجماعات في عصرنا الحاضر. وتختلف المعلومات عن البيانات فالأخيرة هي مجموعة من الحقائق أو القياسات أو المعطيات التي تتخذ صورة أرقام أو حروف أو رموز أو أشكال خاصة، وتعبّر عن فكرة أو موضوعا أو حدثا أو هدفا معينا، لذا توصف بأنّها المادة الخام التي يتم تحويلها عن طريق الحاسوب لغرض استخراج معلومات معينـــة، وتسمـــى العلاقـــة بيـــن المعلومـــات والبيانات بـــ "**الدورة الاسترجاعية**"، إذ يتم تجميع وتشغيل البيانات للحصول على معلومات، ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول معلومات إضافية يعتمد عليها في إصدار قرارات جديدة[25].

يجب أن تتصف المعلومات الجيدة بالخصائص التالية[26]:

- **الوقتية:** وهي تشير إلى أنّ المعلومات يجب أن تتوافر في الوقت المناسب.
- **الإيجاز:** حيث أنّ تلقي المستخدم لمعلومات موجزة، سيوفر عليه الوقت ويمكن الوصول للإيجاز عبر تلخيص البيانات ذات الصلة.
- **الشمولية:** وهي أن تحتوي المعلومات كل البيانات المطلوبة لاتخاذ القرار.
- **الدقة:** وهي نسبة المعلومات الصحيحة إلى المجموع الكلي من البيانات المعالج خلال فترة محددة.

- **التناسبية:** وتعني أن المعلومات تعطى على قدر الصلاحيات، وبقدر من الحاجة لها.
- **الوضوح:** وتعني أنّ المعلومات يجب أن تقدم بهيئة واضحة ومقروءة.
- **يمكن الوصول إليها:** أي أنّه يمكن الوصول للمعلومة عندما نحتاجها وبالشكل الذي نريده.
- **قابلة للتحقيق:** بمعنى أن تكون المعلومات واقعية يمكن تحقيقها، أي أنّه ليس هناك صعوبة في تحقيقها.
- **الحيادية:** بمعنى أن تكون المعلومات خالية من أي تحيّز أو مآرب شخصية وأن تعكس الأحداث والنشاطات بطريقة عادلة ومهنية.
- **لها قيمة تنبؤية:** بمعنى أنّ المعلومة مفيدة لمتخذ القرار كي يتنبأ بمآل الحال التي سيتم اتخاذ القرار بشأنه.
- **لها قيمة رقابية:** بمعنى أن تكون المعلومة مفيدة لمتخذ القرار للرقابة والتقييم من خلال عمليات التغذية العكسية وتصحيح الأخطاء التي يمكن أن تنتج عن سوء الاستخدام أو عدم الكفاءة.

2- مفهوم الأمن المعلوماتي

قبل التطرق إلى مفهوم "الأمن المعلوماتي"، يجب أن نشير إلى مفهوم "**تقنية المعلومات**": فهي نظم تشغيل وتقنيات اتصال وبرمجيات متطورة تسهم في دعم إمكانات الحاسب الآلي بأساليب متطورة، تعتمد على العلم والخبرة والمعرفة وتوفر الوقت والجهد والتكلفة، وأقصى قدر من الدقة لتغذية ومعالجة وتخزين وبث واستخدام ونقل المعلومات والبيانات وحمايتها، وعموما ترتبط تقنية المعلومات على العناصر التالية[27]: تغذية ومعالجة وتخزين وبث استخدام المعلومات، تعتمد على العلم والمعرفة والخبرة، استخدام تقنيات الحاسب الآلي والاتصالات، توفير الجهد والوقت والتكلفة، تتكون من الأجهزة ونظم التشغيل والبرامج وتتمتع بقدر كبير من الدقة.

أمّا عن مفهوم "**الأمن المعلوماتي**" فهو من ***الزاوية الأكاديمية***، يُقصد بأمن المعلومات العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهدّدها، ومن أنشطة الاعتداء عليها، ومن ***الزاوية التقنية***، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الدّاخلية والخارجية، ومن ***الزاوية القانونية***، فالأمن المعلوماتي هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية، التي تستهدف المعلومات ونظمها[28].

كما يُعرف أيضا الأمن المعلوماتي على أنّه: "**مجموعة من الإجراءات الإدارية والفنية التي صُممت لضمان حماية الأجهزة وملحقاتها والبرامج والبيانات من السرقة، أو التوقف أو التلف المتعمد أو غير المتعمد أو التخريب، أو التبديل أو مجرد الإطلاع دون تصريح بالاستخدام، وحماية شبكة المعلومات الداخلية والاتصالات الخارجية من الاختراق أو التعطيل المتعمد أو غير المتعمد**"[29].

ولا يمكن أن يتحقق أمن المعلومات دون توفير الحماية المتكاملة لقطاعين مهمين، عبر معايير أمنية تكفل توفير هذه الحماية، لذا يشمل أمن المعلومات[30]:

- **أمن الاتصالات:** ويراد بأمن الاتصالات حماية المعلومات خلال عملية تبادل البيانات من نظام إلى آخر.
- **أمن الكمبيوتر:** ويراد به حماية المعلومات داخل النظام بكافة أنواعها وأنماطها، كحماية نظام التشغيل وحماية برامج التطبيقات، وحماية برامج إدارة البيانات وحماية قواعد البيانات بأنواعها المختلفة.

المحور الخامس: مهددات الأمن المعلوماتي وأثرها على الأمن القومي

في ظل تطور المعلوماتية، تنامت معه مصادر التهديدات التي توجه أمن المعلومات، والتي كان لها تأثير سلبي كبير على الأمن القومي للدّول.

أولا: أنواع التهديدات الالكترونية لأمن المعلومات

هناك وسائل وأساليب متعددة في اختراق الأمن المعلوماتي للمواقع الالكترونية وهي[31]:

- **صناعة نشر الفيروسات:** والهدف من ذلك تغيير المعلومات في جهاز الضحية، أو حذفها، أو سرقتها ونقلها إلى أجهزة أخرى.
- **القرصنة المعلوماتية:** ويُقصد بها سرقة المعلومات من برامج وبيانات بصورة غير شرعية، وهي مخزنة في دائرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية، وتتم هذه العملية إمّا بالحصول على كلمة السر، أو بواسطة التقاط الموجات الكهرومغناطيسية بحاسيبة خاصة، ويمكن وضعها في عجلة صغيرة أو مكان قريب من مركز إرسال هذه الموجات.
- **تعطيل الأجهزة:** حيث تتم دون عملية اختراق فعلية، بل يكون بإرسال كم هائل من الرسائل بطرق فنية معينة، فيؤدي ذلك إلى تعطيل الأجهزة أو الشبكات وإعاقتها عن عملها.
- **انتحال الشخصية:** وهي جريمة الألفية الجديدة في أمن المعلومات حسب المختصين، وتتمثل باستخدام شخصية أخرى بطرق غير شرعية، وذلك بهدف الاستفادة من المكانة الاجتماعية لإخفاء هوية مجرم.
- **المضايقة والملاحقة:** وتتم إما بالبريد الالكتروني، أو بوسائل الحوارات الآنية، وذلك بإرسال رسالة تهديد وتخويف ومضايقة.
- **التغرير والاستدراج:** وغالبا ما يكون الضحية من هذا النوع هم صغار السن، حيث يوهم المجرم الضحية بأنّه يقيم علاقة صداقة على الانترنت، والتي قد تتطور إلى لقاء مادي بين الطرفين، والمجرمون على الانترنت يتجاوزون الحدود الجغرافية.
- **التشهير وتشويه السمعة:** حيث يقوم المجرم بتسوية سمعة الضحية سواء كان فردا أو جماعة أو مؤسسة تجارية وغيرها، والوسيلة الأهم لهذه الجريمة هو إنشاء

موقع على الانترنت يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.

- **صناعة نشر الإباحية:** لقد وفرت الانترنت الإباحية بشتى وسائل عرضها سواء صور، أو فيديو أو حوارات، وهذا الجانب من أخطر الجرائم وخاصة لمجتمعات محافظة دينيا كالمجتمعات العربية والإسلامية.
- **النّصب والاحتيال:** حيث أنّ الانترنت مجالا رحبا لعرض المنتجات التجارية، بالتالي أصبح بإمكان المحتالين والنصابين عرض منتجات وهمية، وميزة هذه الجريمة سهولة اختفاء وتلاشي المجرم.

تعتبر "**عملية القرصنة المعلوماتية Haking**" بواسطة الحاسوب حجر الأساس الذي ترتكز عيه استراتيجية الهجوم المعلوماتي، فهي تتيح للمتخصصين: إمكانية التجسس على أهداف الخصم، سرقة حجم كبير من سيل المعلومات بشتى مستوياتها، وإقحام معلومات مزيفة في البنية التحتية للمعلومات الوطنية للخصم لبث روح الهزيمة، خلخلة القاعدة التي تستند إليها القرارات الاستراتيجية لقيادة الخصم وكف جملة من الأنشطة الحيوية للبلد التي تستند إلى الحاسوب، كأداة العصر عن طريق أسلحة معلوماتية متخصصة كالفيروسات وغيرها[32].

ويتولّ عملية القرصنة أشخاص هواة أو محترفين، تم تعريفها كالتالي: "هم أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي والشبكات، بحيث تكون لهم القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات أو الشبكات"، ويُصنّف المخترقون إلى نوعين: "**الهاكرز HAKERS**"، وهم الأشخاص الذين لهم القدرة الفائقة على اختراق الأجهزة والشبكات، امّا "**الكراكرز CRACKERS**" فهؤلاء يُطلق عليهم المخربين[33]. ومن أخطر آليات القرصنة المعلوماتية، استخدام ملفات "**أحصنة طروادة Trojan horses Program**"، ويتم بإرسال برنامج التجسّس هذا من قبل المستفيد إلى جهاز الضحية، ليكون حلقة

الوصل بين جهاز الضحية والمخترق أو المستفيد، ويعتبر هذا البرنامج من البرامج الخطرة التي تستخدم في عمليات القرصنة المعلوماتية[34].

وقد شاع استخدام عمليات القرصنة في تنفيذ مثل هذه الاختراقات، لتوفر أكثر من مبرر للدور الفاعل الذي تلعبه، وستلعبه عملية القرصنة المعلوماتية في دائرة الهجمات والتهديدات المعلوماتية، منها: انتشار توظيف الحواسب في إدارة بيانات البنية التحتية الوطنية، تنتقل المعلومات بين الحواسب بعيدا عن المراقبة المباشرة للجهات المستفيدة، عبر شبكة من أقنية الاتصالات، والمعالجات، مما يتيح لقراصنة المعلومات التلصص عليها، دون انتباه الجهات المستفيدة من هذه الخدمة، لا تحتاج أنشطة قرصنة المعلومات إلى مبالغ استثمارية عالية، كما أنّ طبيعة الأجهزة المستخدمة لتحقيق هذا الغرض متاحة في السوق المحلية، ولا تتصف بخصوصية أو تقنية عالية، سهولة مباشرة القرصنة المعلوماتية من أي موقع على الشّبكة، دون الحاجة إلى قواعد الهجمات العسكرية التقليدية[35].

تاريخيا، ترجع بداية القرصنة إلى الستينات، إذ ارتبط ظهورها مع ظهور أولى الحواسيب، إلاّ أنّ أول عملية قرصنة قد سُجلت في عام 1878، بإحدى شركات الهاتف المحلية الأمريكية، ويعتبر الخبراء الفترة من 1980 إلى 1989 العصر الذهبي للقرصنة، وأشهر حروب النت على الإطلاق هي "حرب الهاكرز العظمى" التي دارت بين عامي 1990م و1994م بين فريقين من الهاكرز المحترفين، كما شهد عام 2000م أول حرب إلكترونية دولية بين العرب والمسلمين ضد اليهود وكان نتيجتها اختراق وتعطيل الكثير من المواقع الإسرائيلية، كما شهدت الهند مصيراً مماثلا من قبل الهاكرز الباكستانيين، وكذلك الحرب الأمريكية الصينية عام 2001، بسبب أزمة طائرة التجسس الأمريكية في الصين، والتي راح ضحيتها الكثير من المواقع والشبكات، ومن أشهر القراصنة: الأمريكي "**كيفن ميتنيك**"، وكذا قرصان أطلق على نفسه "**The Menetor**"، والذي قام بنشر دراسة شهيرة بعد أن

تم اعتقاله، أصبحت تعرف باسم "بيان الهاكر"، وهو بيان رسمي لأهداف ووجهات نظر القرصان، وتعتبر أهم ما كُتب عن قرصنة الحاسوب[36].

وتعود أسباب ودوافع حدوث مثل هذه الاختراقات والجرائم المعلوماتية، إلى[37]:

– التنافس السياسي والاقتصادي بين الدول من خلال اختراق قراصنة كل دولة للأنظمة المعلوماتية المعلوماتية للدول الأخرى بهدف التجسس ولأهداف أخرى خفية.

– التسابق القضائي والعسكري بين الدول، فقد قام القراصنة باختراق شبكات معلوماتية تابعة لوكالة الفضاء ناسا، ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الأمريكية.

– كما وُجدت مجموعات تطلق على نفسها مجموعات الكراهية على الانترنت تزدري كل القيم الدينية والأخلاقية والاجتماعية السائدة في المجتمعات، وهناك مواقع الإلحاد التي تطالب بإلغاء الدين والدولة والأسرة وتحرير الإنسان من تلك القيود.

إنّ تبني التوجه نحو مجتمع المعلومات، وتشييد بنية معلوماتية قومية واسعة المجال، نقل المجتمع والدّولة والمؤسسات إلى مرمى المخاطر، وحتّم عليها مواجهة التحديات الشاملة والواسعة النّطاق في أمن المعلومات، بمعنى أنّ تحديات أمن المعلومات في مجتمع يمتلك بنية معلوماتية واسعة، يجعله يواجه تهديدات في أمن المعلومات، تتسم بالشمول والاتساع وعمق التأثير، وتنوع الأدوات وتعدد مصادر الهجوم وأدواته، وغزارة الأهداف التي تشكّل إغراء ومناطق جذب لمن يستهدفونه[38].

بالتالي تأثر مفهوم تحقيق "الأمن القومي" للدول، بحيث تغيرت أشكال التهديدات بظهور نوعية جديدة من التهديدات الأمنية التي لم تكن معروفة من قبل، أبرزها: التهديدات الأمنية لنظم المعلومات وإمكانية ممارسة أعمال القرصنة المعلوماتية بأبعادها المختلفة، فمع ازدياد الاعتماد على نظم المعلومات والحاسب الآلي في

تسيير الأعمال، فإنّ إمكانية اختراق هذه المنظومة من شأنه أن يخلق تهديدات أمنية خطيرة، كالتأثير على حركة الطيران، والمعاملات من خلال ميكانيزمات التجارة الالكترونية، وأعمال البنوك وغيرها من المؤسسات التي تستخدم الأساليب الآلية الحديثة في المعاملات، هذا بالإضافة إلى إمكانية اختراق منظومات المعلومات الأمنية للأجهزة المختلفة، فضلا عن إمكانية اختراق منظومات الاتصال والتحكم المستخدمة لإدارة العمليات[39].

ونتيجة لتوسع استخدام شبكة الانترنت، ظهرت ظاهرة "الإرهاب الشبكي Cyber terrorism"، ويُعرف أيضا بالأمن الالكتروني، والذي يستهدف الأمن القومي الدولي، وخصوصا في مجال التكنولوجيا، إذ أضحت المعادلة التي تجمع قطاعات الكهرباء والاتصال والكمبيوتر من الركائز الضرورية للأمن الاجتماعي والأمن القومي، غذ نجد أنّ معظم الجرائم الإرهابية صارت مرتبطة بالانترنت ففريق إرهابي يقتل، والثاني المتطرف يحرّض ويجنّد، الأمر الذي ساهم في اندثار الحدود بين الإرهاب بمفهومه القديم والإرهاب الالكتروني الذي أصبح تهديدا في كل مكان، مثلا اقتحام صفحة لمستشفى ما وتهديد حياة المرضى عن طريق تغيير برنامج العلاج، ومن الممكن تهديد الاقتصاد باقتحام مواقع البورصة العالمية والمحلية، كما يمكن أيضا التدخل في نظام الاتصالات، الكهرباء والمياه، بل والسيطرة على نظام المواصلات والطيارات، وبذلك تهديد بلد بأكملها، وإن وصل الأمر للتحكم في الشبكات الحكومية وشبكات الأمن وإغلاقها، فستتم السيطرة التامة من جانب الإرهابيين[40]، كما ساهمت الثورة الالكترونية في انتشار المد الإرهابي الفردي بلا قيادة، بعد أن أصبح من السّهل على أي مجموعة أو حتى فرد أن يتعلّم كيف يصنع قنبلة من خلال الانترنت[41].

تعرف دول العالم حاليا تهديدات رقمية متقدمة، مما يطرح إلى الواجهة أهمية الأمن المعلوماتي، ليصبح تحديا رئيسيا ليس للشركات الكبرى فحسب، بل أيضا على مستوى الدول، مثلا منطقة الشرق الأوسط كانت في السنوات الأخيرة مسرحا

لبعض التهديدات الرقمية المتطورة غير المسبوقة، وحروب إلكترونية لم يشهدها أي مكان آخر في العالم، ومن الأمثلة على هذه التهديدات المتطورة والمتنامية "**هجوم ستكسنت**" على عمليات الطرد المركزي النووي في إيران، وهجمات "شامون" على شركات الطاقة في السعودية وقطر.

هذه التهديدات كانت ذات أهداف محددة، ولها تأثير أوسع على المستقبل الاقتصادي أو السياسي للدول المتضررة، الأمر الذي يقودنا إلى القول بأن الحرب الرقمية هي في وقتنا الراهن حقيقة واقعة، خصوصا في ظل الاستخدام المتزايد لعمليات الاختراق من قبل ناشطين مدنيين تعبيرا عن خطاب سياسي أو اجتماعي وهو أحد آثار "الربيع العربي"، ودافع أساسي للهجمات الأخيرة على شركات الخدمات المالية في دول الخليج العربية[42].

يرى "**دافيد هيلد David Held**" أنّ الثورة المعلوماتية التي كرستها العولمة غيرت من نمط خوض الحروب، فانتقلنا من التحريك الفيزيائي للمجتمعات إلى سياسة العلاقات العامة، باستعمال وسائل الإعلام لتعبئة الرأي العام لأنّ أساس الحروب هو الثقة السياسية أولا، حيث يتوافق هذا الافتراض مع الطبيعة الجديدة للحروب التي أصبحت تولي أهمية كبرى للعناصر الثلاثة: التنظيم والتخطيط والتعبئة، مثلما منحت الثورة التقنية التكنولوجية في الميدان العسكري هامشا واسعا في طريقة استخدام القدرات العسكرية بشكل أكبر وبنتائج أدق لخدمة الأهداف المرجوة من العمل العسكري[43]، فحروب المعلومات يمكن أن تلحق الدّمار خاصة بقطاعات حساسة للغاية، كقواعد البيانات الحيوية والمعلومات الاستراتيجية المتعلقة بالأمن القومي للدولة، وقد يستحيل إصلاحها إن أُعطبت، وتُجرى حاليا داخل مختبرات أبحاث معنية بابتكار أسلحة الحرب المعلوماتية وتطويرها، ومن أبرز خصائص حروب الدّمار المعلوماتي أنّ في إمكانها تخطّي الروادع كافة، التي حالت حتى الآن دون نشوب حروب الدّمار الشامل بأسلحتها الراهنة[44].

لقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم حوالي 50 ألف جريمة واعتداء في الساعة، وباتت جرائم المعلومات أدواة جديدة في الصراع السياسي والاقتصادي بين الدول، على سبيل المثال فيروس **دوكو(Duqu)** الذي تم اكتشافه، وغرض تصميمه هو جمع المعلومات الاستخباراتية، والبحث عن وثائق التصميم التي يمكن أن تساعد في المستقبل شن هجومات على منشآت التحكم الصناعي، ويمثّل دوكو الجيل الأحدث من **ستكسنت(Stuxnet)** الذي ذكرت تقارير عديدة أنّ الأمريكيون استخدموه في إحداث فوضى داخل البرنامج النووي الإيراني[45].

وفي الأخير، يمكن إجمال تهديدات ومخاطر الجرائم الالكترونية المستحدثة على الأمن القومي، سياسيا واقتصاديا واجتماعيا وأمنيا، في النقاط التالية[46]:

- جسامة الأضرار الناجمة عنها (البشرية والمادية والتقنية)، بل ووصلت في بعض الدول وخاصة العربية في السنوات الأخيرة، إلى انقلاب أمني واقتتال داخلي وانقسامات داخل هذه المجتمعات.

- انعكاساتها السلبية على البنية الاقتصادي للدولة والمؤسسات والأنشطة الاقتصادية المتعلقة بجذب الاستثمارات الخارجية، نتيجة لضعف الأمن وعدم الاستقرار.

- تمثل خطرا على الاستقرار الأمني.

- تسبب حالة من الاضطراب الاجتماعي لما تدخله من خوف في نفوس الكثير من الأفراد.

- تؤدي إلى فساد الموظفين وبعض الشرائح الاجتماعية بالمجتمع.

- تعمل على إفساد والحد من الاستفادة المطلوبة من التقنيات الحديثة، حيث تصل في بعض الدول إلى قطع الاتصالات بالانترنت، سواء بواسطة أجهزة الدّولة السيادية، أو عن طريق الأعمال الإرهابية التي تقوم بها أفراد أو جماعات تقطع وسائل الاتصالات الدّولية المارة داخل هذه الدول.

المحور السادس: استراتيجيات حماية الأمن المعلوماتي والجهود الدولية للحد من المخاطر المعلوماتية

معلوماتيا، تم استحداث مجموعة من التطبيقات والاجراءات لحماية المعلومات من الاختراقات، أما قوميا فقد بُذلت مجموعة من الجهود الدولية العربية وإن كانت قليلة، في مجال التنسيق الأمني المعلوماتي للتصدي للتهديدات الأمنية المعلوماتية

أولا: استراتيجيات حماية الأمن المعلوماتي

تنضوي المعلومات على أهمية وقيمة مادية ومعنوية للأفراد والشركات والدول وتزداد أهميتها في المنظمات الأمنية والعسكرية والاقتصادية ذات الطابع الاستراتيجي، لهذا ارتبط عنصر السرية بالمعلومات ودرجة توافرها في ضوء ما يترتب عن فقدانها من خسائر، وما يترتب على توافرها من مكاسب، حيث تلعب دورا مهما في انتصار وهزيمة الدول[47]، لذا وجب وضع مجموعة من الاجراءات الوقائية للتصدي لأخطار التهديدات والاعتداءات على المعلومات أو ما يُعرف بـــ "الأمن المعلوماتي"، وهي كالتالي[48]:

- ❖ **خدمات (وسائل) حماية التعريف Identification and Authentification**: وتهدف هذه الخدمات إلى التثبت من الهوية، ويعد التعريف من الوسائل التي تحمي من أنشطة التخفي والتنكر، وهناك نوعين من خدمات التعريف، الأول تعريف الشخصية وأشهر وسائلها كلمات السر، وثانيها التعريف بأصل المعلومات كالتثبت من أصل الرسالة.

- ❖ **خدمات (وسائل) السيطرة على الدخول Access Control**: وتستخدم هذه الخدمات للحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، ولهذا فإنّ خدمات التحكم بالدخول تعد الوسائل الأولية لتحقيق التخويل والتثبت منه.

❖ **خدمات (وسائل) السرية Data and message confidentiality:** تسمح هذه الخدمات بحماية المعلومات من الإفشاء للجهات غير المصرح لها بالحصول عليها، والسرية تعني بشكل عام إخفاء المعلومات من خلال تشفيرها.

❖ **خدمات (وسائل) حماية التكاملية وسلامة المحتوى Data and message integrity:** وتهدف هذه الخدمات إلى حماية مخاطر تغيير البيانات خلال عمليات إدخالها أو معالجتها أو نقلها، وعملية التغيير تعني بمفهوم الأمن هنا الإلغاء أو إعادة تسجيل جزء منها أو غير ذلك، وتهدف هذه الوسائل أيضا وتهدف هذه الخدمات إلى حماية مخاطر تغيير البيانات خلال عمليات إدخالها أو معالجتها أو نقلها، وعملية التغيير تعني بمفهوم الأمن هنا الإلغاء أو إعادة تسجيل جزء منها أو غير ذلك، وتهدف هذه الوسائل أيضا إلى الحماية من أنشطة تدمير المعطيات بشكل كامل أو إلغائها دون تخويل.

❖ **خدمات (وسائل) منع الإنكار Non-repudiation:** وتهدف هذه الخدمات إلى منع الجهة التي قامت بالتصرف من إنكار حصول نقل البيانات أو النشاط من قبلها.

كما وُجدت العديد من التطبيقات، التي يمكن أن تساعد على الحد من التهديدات المعلوماتية التي نسمع بها في وقتنا الحالي، ومن بينها:

- **نظام تحديد الأماكن العالمي:** وهو عبارة عن منظومة إلكترونية متكاملة تعمل بواسطة أجهزة صغيرة، تقوم باستقبال إشارات معينة صادرة عن عدة أقمار صناعية، يتم من خلالها تحديد الموقع على وجه الدقة، مما يساعد على التدخل وتحديد الإجراءات المطلوبة في مراحل الأزمة.
- **نظم المعلومات الجغرافية:** وتعتمد هذه النظم على استخدام البيانات المرتبطة بمواقع جغرافية معينة، ويستعان في تشغيل هذه النظم بالخرائط الرقمية والصور الملتقطة بالأقمار الصناعية، ويتيح هذا النظام التعرف على أماكن البؤر الإجرامية.

• **استخدام المحاكاة الحاسوبية في إدارة الكوارث والأزمات:** من خلال الاستفادة من قدرات الحاسبات الآلية على تشغيل برامج تحوي نماذج تفصيلية لأنظمة واقعية كالمنشآت والأحياء السكنية، ثم افتراش حالات للطوارئ، بما يمكن الأجهزة والكوادر الأمنية المختصة من وضع الخطط الكفيلة للسيطرة على أي خلل، واتخاذ إجراءات وتدابير الوقاية والتأمين.

• **رصد وتتبع الأنشطة الإجرامية على الانترنت:** وذلك من خلال إنشاء وحدات متخصصة، مزودة بالأجهزة والمعدات التكنولوجية المتطورة، يُناط بها رصد ومراقبة المواقع المشبوهة على شبكة الانترنت.

• الكشف عن شخصية مرتكبي الجرائم آليا: عن طريق استخدام الحاسب الآلي في استخراج صحيفة الحالة الجنائية بالأحكام النهائية الصادرة ضد الأشخاص، وحفظ صور البصمات والتعامل بها بصورة علمية منظمة، من خلال إنشاء أرشيف إلكتروني لحفظ البصمات.

• **إنشاء قاعدة بيانات ذات صلة بالجرائم الاقتصادية:** من خلال استخدام الحاسبات الآلية في حفظ وتصنيف المعلومات والبيانات ذات الصلة بالجرائم الاقتصادية ومُرتكبيها، مع استخدام الأرشيف الالكتروني (بيئة رقمية).

• **إنشاء غرف عمليات متطورة:** بتزويدها بأحدث أجهزة الاتصالات السلكية واللاسلكية الالكترونية، وربطها بالأجهزة الأمنية المختصة لنقل وتبادل المعلومات ودعم اتخاذ القرار، وإنشاء غرف عمليات حديثة لإدارة الكوارث وتزويدها بنظام **(G.I.S)** والحاسب الآلي للتعرف على موقع الحدث.

• **تأمين المنشآت إلكترونيا:** من خلال توفير شبكات للاتصال ونقل وتبادل المعلومات على مستوى تكنولوجي متطور، للربط بين الأجهزة الأمنية المختصة بتأمين المواقع والمنشآت السياحية والاقتصادية ومختلف الأنشطة الحيوية[49].

في ظل الأهمية التي يلعبها أمن المعلومات في العالم، أصبح حماية الشركات والمؤسسات من الحوادث الأمنية واقع ملح، مثل: تشويه المواقع، تسريب البيانات

وعليه تم استحداث بعض المعايير العالمية وبعض القوانين المرتبطة بأمن المعلومات، أهمها[50]:

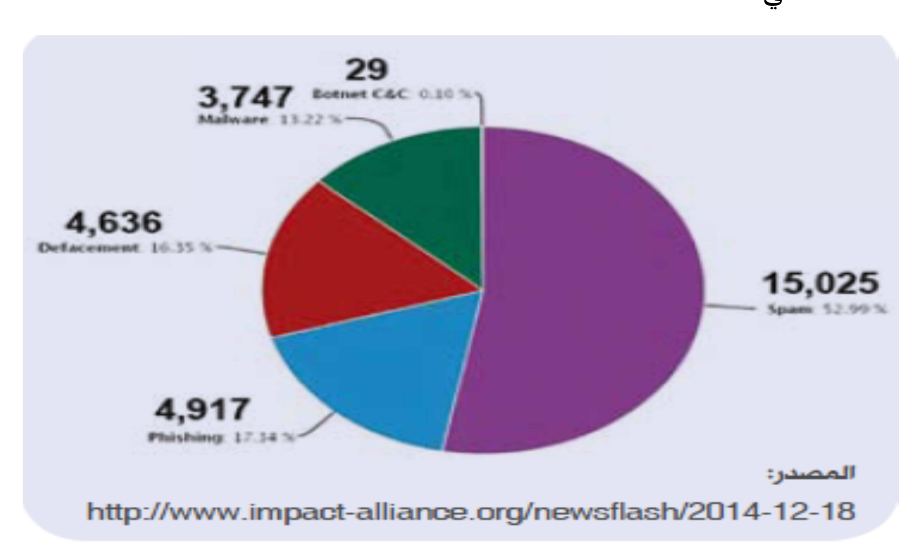
- **<u>معايير الأيزو:</u>** المنظمة الدولية للتوحيد ايزو Iso، الذي أنشئ عام 1947 وهو هيئة غير حكومية تتعاون مع اللجنة الدولية الكهروتقنية والاتحاد الدولي للاتصالات، يهتم بصياغة السياسات الأمنية والاتصالات وإدارة العمليات.
- **<u>معيار الكوبيت</u> The Control Objectives for Information Cobit related Technology:** تم إنشاء هذا المعيار من قبل معهد حوكمة تقنية المعلومات عام 1995، وهو عبارة عن إطار للسيطرة أو التحكم، تربط تقنية المعلومات بمتطلبات العمل وتنظيم لأنشطة تكتولوجيا المعلومات، وتحديد الموارد الرئيسية لتكنولوجيا المعلومات وأهداف الرقابة الادارية التي ينتظر منها.
- **<u>معيار ITIL</u> The Information Technology Infrastructure Library:** ويسمى أيضا **أيزو 20000**، وهو عبارة مجموعة من أفضل الممارسات في مجال إدارة خدمات تقنية المعلومات، ويركز علة خدمة عمليات تقنية المعلومات، ويعتبر الدور الرئيسي للمستخدم، تم إنشاؤه بواسطة مكتب المملكة المتحدة لتجارة الحكومة.
- مثلما هناك بعض اللوائح والقوانين التي أصدرتها الولايات المتحدة الأمريكية عام 2002، منها: **قانون SOX** (هدفه حماية المستثمرين عن طريق تحسين دقة وموثوقية نظام التعريف)، **قانون COSO** (يعمل على تحسين السيطرة على الشركات من خلال نظام الرقابة على المعلومات والاتصالات)، **قانون HIPAA** (يعني قابلية التأمين الصحي)، **قانون FISMA** (يعني قانون إدارة امن المعلومات الفيدرالي) وقانون FIPS (معايير معالجة المعلومات الفيدرالية).

ثانيا: بعض الجهود الدولية والعربية للحد من الاختراقات الأمنية المعلوماتية التي تمس بالأمن القومي: تبقى الجهود الدولية والإقليمية في مجال مكافحة الاختراقات الأمنية التي تواجه الأمن القومي للدول، ضئيلة مقارنة بحجم الجرائم والتجاوزات التي تحدث في كل ثانية، كما وأُبرمت العديد من الاتفاقيات غير قابلة للتنفيذ، خصوصا في ظل تنامي الفجوة المعلوماتية بين الدول المتقدمة التي تمتلك التقنية المعلوماتية المتطورة، والدول النامية التي تفتقر لتلك التقنية، كما وأنّ المشكلة تكمن في عدم التنسيق الأمني المعلوماتي على المستوى الدولي، وكيف سيتم ذلك ومعظم الاختراقات المعلوماتية وراءها دول ومؤسسات، لكن بالرغم من ذلك يمكن ذكر بعض الجهود على سبيل المثال لا الحصر، فهي بقيت رهينة خطابات أمنية دون التطبيق.

لقد قامت دول الاتحاد الأوروبي بالإضافة إلى بعض الدول الأخرى مثل الولايات المتحدة الأمريكية في مجال مكافحة الاختراقات والجرائم المعلوماتية وكندا وجنوب افريقيا، بالتوقيع على "**اتفاقية بودابست**" لمكافحة الجرائم المعلوماتية في عام 2001، والتي تنص على أنّ الدول الموقعة على الاتفاقية يجب أن تضع إطار عام للتفاهم والتعاون الدولي لمكافحة جرائم الفضاء المعلوماتي، وتحدد الإجراءات الواجب اتخاذها على المستوى الوطني سواء من الناحية الموضوعية أو الإجرائية لمكافحة الجرائم المعلوماتية، كما تحدّد الإطار العام للتّعاون الدولي الرسمي وآليات الحصول على الأدلة الجنائية الرقمية خارج الحدود، أمّا في المنطقة العربية، فقد تم إعداد قانون استرشادي عربي للجرائم المعلوماتية سمي "**قانون الإمارات العربي الاسترشادي لمكافحة جرائم المعلومات وما في حكمها**" والذي تم اعتماده من قبل جامعة الدول العربية، وذلك بهدف تحفيز إصدار التشريعات اللازمة وتوحيد الجهود في هذا المجال، كما تم التوقيع على "**اتفاقية مكافحة جرائم المعلومات**" لعام 2010 الموقعة بين الدول الأعضاء في جامعة

الدول العربية، والتي تضمن إلزام الدول الموقعة عليها بإصدار تشريعات داخلية لمكافحة جرائم المعلومات[51].

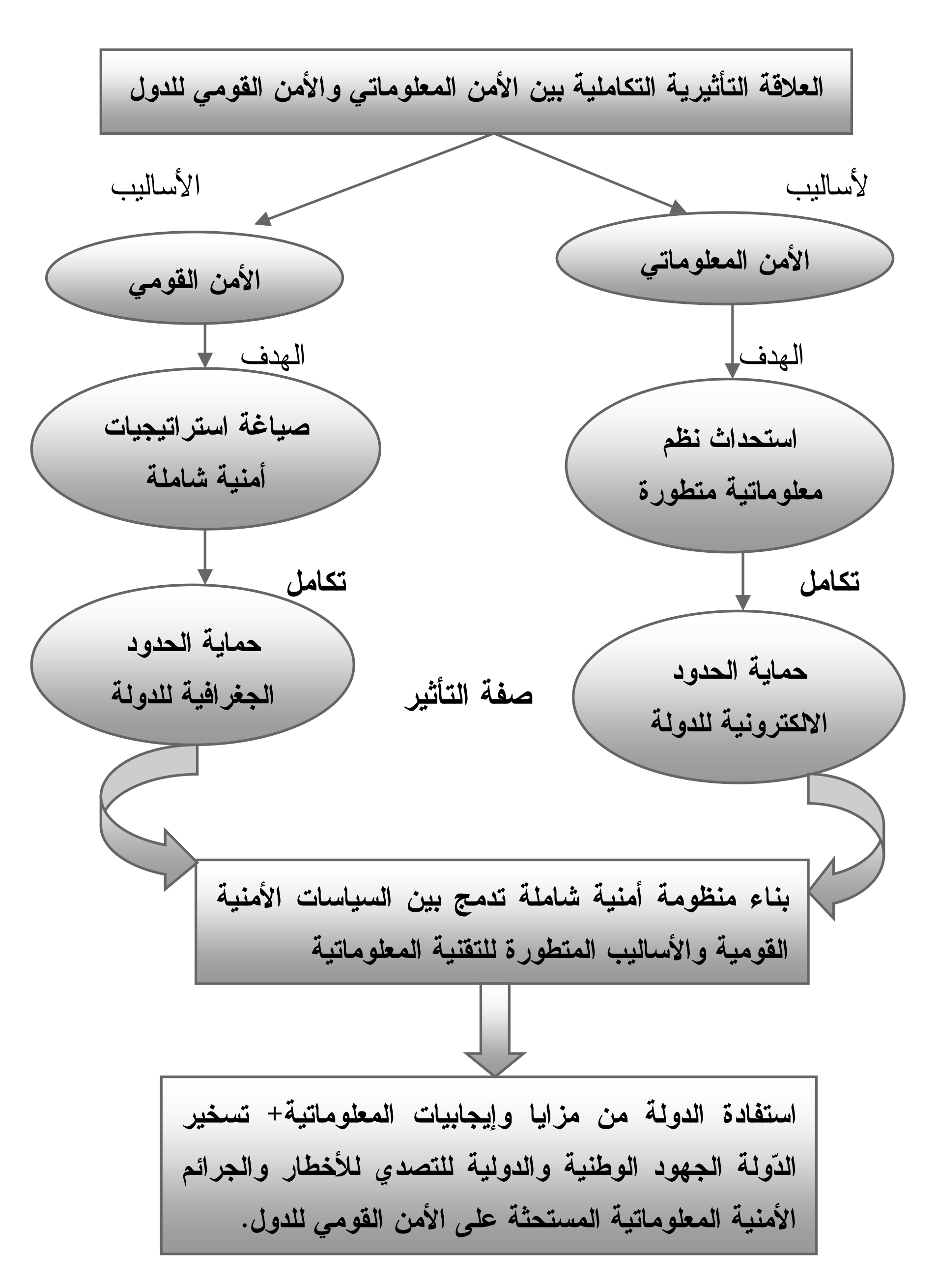
مثلما اهتمت الشراكة الدولية متعددة الأطراف لمكافحة الجرائم السيبيرانية **IMPACT** بالتعاون مع الاتحاد الدولي للاتصالات (الوكالة الدولية المتخصصة بتكنولوجيا المعلومات والاتصالات التابع للأمم المتحدة)، بموضوع الأمن السيبيراني على شبكة الانترنت، وتم التوقيع على" **اتفاقية شراكة**" ما بين الطرفين بهدف تقديم الخبرات ونشر الوعي والإحصائيات المتعلقة بأمن المعلومات عبر الشبكة، وذلك لحماية الافراد والشبكات والمؤسسات من التعرض للتهديدات الأمنية كونها اهتمت بأمن الفضاء السيبيراني فقطن والذي يهتم بأمن المعلومات والحوادث على شبكة الانترنت العالمية، وبحسب التقرير الأسبوعي لـــ IMPACT للفترة ما بين 11-2014/12/17، فإن أكثر التهديدات الأمنية كانت رسائل الواغل Spam يليها حالات التصيد على الشّبكة **Phishing**، ثم حالات التشويه **Defacement**، ثم البرمجيات الخبيثة **Malware**، وأقلها الربوتات البرمجية **Botnet**[52]، وفقا للمخطط التالي:



وأي من تصميم أو بيع أو تداول أو استخدام لمثل هذه التهديدات تعتبر من قبيل الجرائم المعلوماتية التي يعاقب عليها القانون عادة وفق بند "إساءة استعمال الأجهزة أو البرامج المعلوماتية".

لكن، مثل هذه الجهود لا يمكن أن تتحقق إلا وفق رؤى وأسس علمية، لمواجهة الجرائم المستحدثة على الأمن القومي للدول السالفة الذّكر، منها: الاعتماد على المنهج العلمي سواء في التخطيط الاستراتيجي، أو أساليب أداء القطاعات الأمنية المعنية بمكافحة الجريمة، إضافة إلى ذلك تشجيع البحث العلمي في مجال البحوث الأمنية ومنها البحوث الأمنية المعلوماتية، ويجب صياغة استراتيجيات أمنية معلوماتية واقعية وقابلة للتنفيذ على المديين البعيد والمتوسّط.

في الأخير، ونظرا لمختلف التهديدات التي يتعرض لها الأمن القومي للدول (من جراء المخاطر المعلوماتية)، والذي يعتبر الهدف الحيوي لجميع الاستراتيجيات والسياسات الأمنية للدول، لابد على صناع القرار من مواكبة التطورات الراهنة، مع إحداث نوع من التكامل بين استراتيجيات حماية الأمن القومي، واستراتيجيات حماية النظم المعلوماتية المتعلقة بجميع القطاعات الحيوية للدولة، وهو ما سيبيّنه المخطط التالي:



ملاحظة: الشكل من إعداد الباحثة.

خاتمة: النتائج والتوصيات: بالرّغم من الإيجابيات التي عرفها عصر المعلوماتية، وما حققته من طفرة نوعية في مجال استخدام المعلومات، وتطبيق ما يُعرف بـــ "الحكومة الالكترونية"، إلاّ أنّ السّلبيات طغت ببروز إشكالية كبرى على الساحة العالمية، وهي: "الأمن المعلوماتي وكيفية تحقيقه، على إثر تزايد الجرائم المعلوماتية يوما بعد يوم، وساعة بعد ساعة، خصوصا تلك المتعلقة بالقرصنة المعلوماتية.

وهي الميكانيزمات التي أدّت إلى حدوث تحولات مهمة على مستوى إعادة تعريف مصادر تهديد الأمن القومي للدّول في ظل تنامي الاختراقات المعلوماتية بالنّسبة لقواعد البيانات للقطاعات الحيوية للدّول، خصوصاً تلك المتعلقة بالاستخبارات والاقتصاد، كما وقد تمّ استغلال المعلوماتية من قبل شبكات المافيا لتسهيل عملياتهم المستهدفة والتي ترتبط بالجرائم المنظمة والعابرة للأوطان كـــ : غسيل الأموال، الهجرة غير الشرعية، المخدرات، الإرهاب الالكتروني، عمليات التجسس الاستخبارتية...إلخ، وعليه بدل من أن تكون المعلوماتية نقطة قوة للدولة جعلت من الأمن القومي مكشوفا، وأصبحت الدولة في مواجهة تهديدات لا تماثلية مجهولة المصدر، وتشير معظم الرؤى الاستشرافية في الدراسات الاستراتيجية أنّ الحروب المستقبلية ستكون "حروبا معلوماتية" (رقمية)، وقوة تدميرها تفوق أسلحة الدّمار الشامل.

إنّ ما فرضه الواقع الأمن المعلوماتي على الأمن القومي للدول، استلزم وضع تشريعات وسن قوانين محلية ودولية من قبل الدول، وجُسدت جهود دولية واستراتيجيات قومية، إلاّ أنّ ذلك اصطدم بواقع خطير وهو: زيادة ذكاء القراصنة وأصبحت الاختراقات عمليات منظمة من قبل الدول والمؤسسات الأمنية العسكرية، السياسية والاقتصادية.....إلخ، وهو ما سيخلق أزمة أمنية أخرى بالنّسبة لأمن الدول النامية، الغير متمكنة من تكنولوجيا المعلومات، في مواجهة مختلف التهديدات المستحدثة على الأمن القومي للدول.

النتائج: تخلص الدراسة إلى النتائج التالية:

- الأمن ضد الخوف، ويتعلق الأمن القومي بالقدرة السياسية+القدرة الاقتصادية+ القدرة العسكرية+ القدرة الاجتماعية+القدرة المعلوماتية (التكنولوجية).
- يستلزم إدراك طبيعة التهديدات، الإحاطة بتجليات التحولات الدولية المعاصرة، من أجل صياغة وانتهاج السياسات المناسبة.
- ارتبط ظهور إشكالية "الأمن المعلوماتي" بالثورة المعلوماتية، أحد أهم إفرازات العولمة، حيث تشكل المعلومات واحدة من أبرز عناصر القوة المعاصرة بفعل الاستخدام الموسع للشبكات الالكترونية.
- هناك مجموعة من العناصر التي تُكوّن المجتمع المعلوماتي: الحكومة الالكترونية، التجارة الالكترونية، التعليم الالكتروني، التوظيف الالكتروني....إلخ.
- يرتبط مفهوم الأمن المعلوماتي بمجموعة من الاستراتيجيات والتدابير الكفيلة لحماية المعلومات من الاختراقات الالكترونية والجرائم المعلوماتية.
- تسبب استخدام التقنية المعلوماتية في حدوث العديد من التهديدات الأمنية التي طالت جميع القطاعات الحيوية في الدّولة، بالتالي المساس بالأمن القومي بانتشار عمليات الارهاب الالكتروني، وتوسيع شبكات المافيا عبر الانترنت، بروز ما يعرف بالصراعات أو الحروب الرقمية، سياسيا واقتصاديا..، كما تُطرح نقطة حرجة وهي تهديد "الأمن الهوياتي" الذي يشكل أحد ركائز الأمن القومي.
- إنّ رهان تحقيق البعد التكاملي في العلاقة التأثيرية بين الأمن المعلوماتي والأمن القومي للدول، مرتبط بنجاعة:- السياسات والاستراتيجيات الأمنية القومية.
- النظم الأمنية المعلوماتية المستحدثة لكل قطاع من القطاعات الحيوية للأمن القومي.
- قوة التشريعات القانونية لمحاربة الجرائم المعلوماتية +إحكام الرقابة الأمنية المحلية، الإقليمية والدولية.

التوصيات: حاولنا من خلال الدراسة، اقتراح بعض الحلول، وهي كالتالي:

– تطبيق ما يُعرف بحوكمة تكنولوجيا المعلومات، من خلال وضع المعايير والمبادئ الضرورية لصياغة الأهداف ورسم السياسات اللازمة لتحسين عمليات تكنولوجيا المعلومات، مع التشديد على عنصر الرقابة الدورية والمنتظمة.

– تبني منظومة قانونية وتشريعية جديدة للوقاية من تهديدات الجرائم المعلوماتية وتقليصها.

– إنشاء لجان محلية ودولية متخصصة في الأمن المعلوماتي، وملمة بالأمن القومي، لإمكانية تحديد التهديدات بدقة، بالتالي القدرة على وضع استراتيجيات أمنية شاملة وواضحة، واقعية وقابلة للتنفيذ، على اعتبار أنّ الأمن المعلوماتي جزء حيوي من الأمن القومي.

– ضرورة تخصيص الدولة ميزانية معتبرة، لاستحداث نظم وكوادر أمنية متطورة، وكذا إنشاء مراكز التدريب الأمنية المتخصصة.

– إيجاد أطر مفاهيمية ونظرية موحدة بالنسبة لأمن المعلومات بين جميع الدول، ليسهل التعاون الدولي في مواجهة الجرائم والتهديدات المعلوماتية، في إطار تعزيز عقد اتفاقيات دولية وإقليمية، بالرغم من أن ذلك صعب نظرا للفجوة المعلوماتية الموجودة بين الدول المتقدمة والدول النامية ومنها: العربية، والتي عليها بذل جهود حثيثة لامتلاك التقنية المعلوماتية، وتشجيع التعاون الأمني المعلوماتي العربي–عربي.

– علميا: القيام بإعداد المؤتمرات والندوات العلمية، لغرس الوعي المعلوماتي لدى الشباب والمراهقين باعتبارهم الفئة المستهدفة من طرف منفّذي الهجمات المعلوماتية، بالإضافة إلى تطوير البحوث العلمية الأكاديمية في مجال أمن المعلومات.

– تعزيز جهود الانتربول، مع محاولة الدول العربية إنشاء نظام شرطة عربي مجهز بتقنية ونخبة معلوماتية عالية، ليسهّل ذلك التعاون مع الشرطة الدولية لتقليص مخاطر الأمن المعلوماتي.

الهوامش:

1- خالد معمري، **التنظير في الدراسات الأمنية لفترة ما بعد الحرب الباردة دراسة في الخطاب الأمني الأمريكي بعد 11 سبتمبر**، مذكرة ماجستير في العلوم السياسية، جامعة باتنة 2008/2007، ص18.

2- عادل زقاغ، **إعادة صياغة مفهوم الأمن –برنامج البحث في الأمن المجتمعي**، على الرابط الالكتروني التالي: http://politics-ar.com/ar/files/06.pdf، تم الاطلاع عليه بتاريخ: 2015/08/15، على الساعة: 15:06 سا .

3- Barry Buzan, Ole Woever**, regions and powers: the structure of international security**, U.S.A: Camdridge University Press, 2003, p491.

*- أستاذ الدراسات الاستراتيجية والمدير الأسبق لأكاديمية ناصر العسكرية.

4- زكريا حسين، **الأمن القومي**، على الرابط الالكتروني التالي: http://www.khayma.com/almoudaress/takafah/amnkaoumi.htm، تم الاطلاع عليه بتاريخ، 2015/09/09، على الساعة: 02:19 سا

5 – خالد معمري، **مرجع سابق الذّكر**، ص ص 25–27.

6- زكريا حسين، **مرجع سابق الذّكر**.

7- خلود خالد، **الأمن القومي في مصر واستخدامه وعلاقته بحرية تداول المعلومات**، على الرابط الالكتروني التالي: http://www.afaegypt.org، تم الاطلاع عليه بتاريخ: 2015/09/03 على الساعة: 15:09سا.

8- **المرجع نفسه.**

9- وداد غزلاني، مداخلة بعنوان: **تطور مفهوم الأمن في العلاقات الدولية**، الملتقى الدولي الأول حول: المقاربة الأمنية الجزائرية في الساحل الإفريقي، جامعة 08 ماي 1945، قالمة، الجزائر 24–25 نوفمبر 2013، ص 14.

10- عادل زقاغ، **مرجع سابق الذّكر**.

11- وداد غزلاني، **مرجع سابق الذّكر**، ص ص 16–17.

12- سليمان عبد الله الحربي، **مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)**، المجلة العربية للعلوم السياسية، بيروت، العدد 19، 2008، ص 27.

13- محمد سعد أبو عامود، **المفهوم العام للأمن**، على الرابط الإلكتروني http://www.policemc.gov.bh/reports/2011/April/17-4-2011/634386635860127946.pdf، تم الاطلاع عليه بتاريخ: 2015/09/28، على الساعة: 15:15سا.

14- سليمان عبد الله الحربي، **مرجع سابق الذّكر**، ص ص 29-30.

15- محمد البخاري طشقند، **الانترنت ومبادئ الأمن المعلومات**، على الرابط الالكتروني التالي: http://diae.net/4155 تم الاطلاع عليه بتاريخ: 2015/09/05، على الساعة: 14:06سا.

16- سمير ابراهيم حسن، **الثورة المعلوماتية عواقبها وآفاقه**ا، مجلة جامعة دمشق، المجلد 18/ العدد الأول، 2002، ص208.

17- بلال الشافعي، **ثورة المعلومات**، على الرابط الالكتروني التالي: http://www.najah.edu/sites/default/files/Information_Revolution_Newsletter56_57.pdf، تم الاطلاع عليه بتاريخ: 2015/09/01، على الساعة: 14:05سا.

18- ناهد عبد الكريم حافظ، **مخترقةً للحدود وللعقول معاً الثورة المعلوماتية.. وأثرها في تغيير المجتمع**، على الرابط الالكتروني التالي: http://www.almutmar.com/index.php?id=200719736، تم الاطلاع عليه بتاريخ: 2015/09/02، على الساعة: 12:02سا.

19- بلال الشافعي، **مرجع سابق الذّكر**.

20- محمد البخاري طشقند، **مرجع سابق الذّكر**.

21- شعبان فرج، مداخلة بعنوان: **الحكومة الالكترونية، إطارها النظري والمفاهيمي**، الملتقى العلمي الدولي الأول حول "متطلبات إرساء الحكومة الالكترونية في الجزائر: دراسة تجارب بعض الدول"، جامعة سعد دحلب –البليدة-، الجزائر، 13-14 ماي 2013، ص 04.

22- نادية بوضياف بن زغموش، فاطمة مخلوفي، مداخلة بعنوان: **التعليم العالي والبحث العلمي في ظل الثورة المعلوماتية وتكنولوجية الاتصال**، الملتقى الوطني الثاني (الحاسوب وتكنولوجيا المعلومات في التعليم العالي 05-06— مارس 2014)، ص ص 601-602.

23- مليكة عطوي، **الجريمة المعلوماتية**، حوليات جامعة الجزائرI، العدد 21، جوان 2012 ص08.

24- محمد يحياوي، **مخاطر القرصنة المعلوماتية على الحكومة الالكترونية**، مجلة البحوث والدراسات العلمية، العدد الخامس، لمركز الجامعي د. يحيى فارس، المدية، الجزائر، جويلية 2011، ص 268.

25- محمد علي سالم، حسون عبيد هجيج، **الجريمة المعلوماتية**، مجلة بابل، المجلد 14، العدد الثاني، 2008، ص 86.

26- أيمن محمد فارس الدنف، **واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**، مذكرة ماجستير، كلية التجارة، الجامعة الإسلامية، غزة (فلسطين) 2013، ص 28.

27- منصور بن سعيد القحطاني، **مهدّدات الأمن المعلوماتي وسبل مواجهتها**، جامعة نايف العربية للعلوم الأمنية، 2008، ص ص 17-18.

28- فتيحة ليتيم، نادية ليتيم، **الأمن المعلوماتي للحكومة الالكترونية وإرهاب القرصنة**، مجلة المفكر، العدد 12، جامعة محمد خيصر، كلية الحقوق والعلوم السياسية، بسكرة، مارس 2015 ص 239.

29- منصور بن سعيد القحطاني، **مرجع سابق الذّكر**، ص 19.

30- المركز الوطني للمعلومات بالجمهورية اليمنية، **الأعمال الالكترونية وأمن المعلومات**، على الرابط الالكتروني التالي: http://www.yemen-nic.info/contents/Informatics/studies/7.pdf نم الاطلاع عليه بتاريخ: 2015/08/08، على الساعة: 13:00سا.

31- محمد يحياوي، **مرجع سابق الذّكر**، ص ص 268-271.

32- حسن مظفر الرزّو، **الأطر المستقبلية لإعداد ملاكات الأمن المعلوماتي**، على الرابط الالكتروني التالي: http://www.alukah.net/culture/0/5426/، تم الاطلاع عليه بتاريخ: 2015/08/28، على الساعة: 08:14سا.

33- فتيحة ليتيم، نادية ليتيم، **مرجع سابق الذّكر**، ص 242.

34- **المرجع نفسه**، ص 243.

35- حسن مظفر الرزّو، **مرجع سابق الذّكر**.

36- ليتيم فتيحة، ليتيم نادية، **مرجع سابق الذّكر**، ص ص 242-243.

37- مليكة عطوي، **مرجع سابق الذّكر**، ص 10.

38- جمال محمد غيطاس، **الأمن المعلوماتي والجرائم المعلوماتية. أدوات جديدة للصراع**، مركز الجزيرة للدراسات، الدوحة، 2012، ص ص 04-05، على الرابط الالكتروني التالي:

http://studies.aljazeera.net/ResourceGallery/media/Documents/2012/2/29/2012229132153559580Information%20security%20and%20cyber%20crime.pdf

39- محمد سعد أو عامود، **مرجع سابق الذّكر**.

40- عبد الحميد إبراهيم محمد العريان، **العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة: ما هو رد فعل القطاع الخاص**، من: الدورة التدريبية حول: مكافحة الجرائم الإرهابية المعلوماتية خلال الفترة: 9-2006/04/13، القنيطرة، المغرب، 2006، ص ص 02-03.

41- محمد جمال الدين مظلوم، ورقة علمية بعنوان: **تأثير الجرائم المستحثة على الأمن القومي** في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدّولية، عمان 2-2014/9/4، ص 09.

42 ميغا كومار، **هل الأمن المعلوماتي في الشرق الأوسط يحتاج للتجديد؟** على الرابط الالكتروني التالي: https://www.alarabiya.net/servlet/aa/pdf/dca1324d-141a-43e5-b209-a86983109015 ، تم الاطلاع عليه بتاريخ: 2015/09/04، على الساعة: 12:00سا.

43- خالد معمري، **مرجع سابق الذكر**، ص69.

44- اسماعيل صبري مقلد، **ثورة المعلومات وحروب المستقبل المحتملة**، مجلة آفاق المستقبل العدد 15، الإمارات العربية المتحدة، جويلية/أوت/سبتمبر 2012، ص 42.

45- جمال محمد غيطاس، **مرجع سابق الذّكر**، ص ص02-03.

46- محمد جمال الدين مظلوم، **مرجع سابق الذّكر**، ص ص 15-16.

47- منصور بن سعيد القحطاني، **مرجع سابق الذكر**، ص20.

48- المركز الوطني للمعلومات بالجمهورية اليمنية، **مرجع سابق الذكر**.

49- محمد علي قطب، **المواجهة الأمنية الآنية للجرائم المعلوماتية**، على الرابط الالكتروني: http://www.policemc.gov.bh/reports/2010/October/8-10-2010/634221514879164114.pdf ، تم الاطلاع عليه بتاريخ: 2015/08/12، على الساعة: 17:05 سا.

50- فهد فايز المدرع، **المعايير العالمية لأمن المعلومات**، على الرابط الالكتروني التالي: http://faculty.mu.edu.sa ، تم الاطلاع عليه بتاريخ: 2015/09/07، على الساعة: 14:09سا.

51- فاديا سليمان، **الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية**، مجلة الدراسات المالية والمصرفية، العدد الأول، 2015، الصادرة عن الأكاديمية العربية للعلوم المالية والمصرفية، الأردن، ص 08.

52- **المرجع نفسه**، ص 09.

تقنيات التّعايش الإلكترونيّ مع الفيروسات لتأمين الملفات الإلكترونيّة

أ. ياسين بوراس
جامعة مولود معمري، تيزي–وزو

مقدمة: تُعدُّ الفيروسات الإلكترونيّة مشكلة مهدِّدة للمعلومات الّتي تُحفَظَ على شكل ملفات إلكترونيّة في الحواسيب، والأقراص الصّلبة، والأقراص المَرِنة والأقراص المضغوطة، والأقراص الضّوئيّة، وبطاقات الذّاكرة، باعتبارها وسائل للتخزين الإلكترونيّ والنّقل المعلوماتيّ، وهي مشكلة تضطّر مستخدمي هذه الأجهزة الإلكترونيّة في تخزين المعلومات ونقلها، إلى التّردّد على محلات إصلاح الحواسيب؛ لتأمين ملفاتهم أو استعادتها، أو تؤدِّي بهم إلى فقدانها نهائيًّا، بسبب عدم معرفة التّعامل مع مهدِّدات الفيروسات. وعلى هذا الأساس جاء بحثنا في هذا الموضوع منصبًّا، على بيان طريقة التّعايش الإلكترونيّ مع مثل هذه المهدِّدات الإلكترونيّة، الّتي تُؤثِّر على الحياة العلميّة والعمليّة للمتعاملين مع أجهزة الحاسوب والتّخزين المعلوماتيّ، في حفظ الملفَّات الإلكترونيّة ونقلها. ولكون بعض تقنيات التّعامل مع الفيروسات معروفة من النّاحية العمليّة أو التّطبيقيّة، إلا أنّها غير معروفة من ناحية التّوثيق باللّغة العربيّة، فإنّ بحثنا في هذا الموضوع إن لم يكن مِنْ قَبِيل الاكتشاف، فعسى أنْ يكون من قَبِيل التّوثيق باللّغة العربيّة، للإضافة إلى رصيدها اللّغويّ بعضا من النّصوص العلميّة حول علم المعلوماتيّة.

أولا– تعريف الملفّ الإلكترونيّ: هو مجموعة من المعلومات الّتي تم تخزينها على الحاسوب بصيغة معيّنة على شكل نص، أو عرض تقديميّ، أو جدول، أو صورة، أو مقطع موسيقى، أو فيديو، أو برنامج تطبيق. والذي يكون متاحاً لبرامج الحاسوب معالجته عن طريق وسيط (جهاز) تخزين معيّن. ويمكن اعتبار ملفَّات

الحاسوب النّظير الحديث للمستندات الورقيّة المستخدمة في المكاتب؛ وهذا هو أصل تسميتها بـــالملفات[1].

أنواع الملفّات الإلكترونيّة



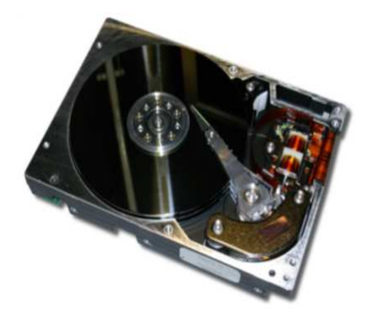
(docx.نصّ) (ppt.عرض تقديميّ) (xlsx.جدول) (jpg.صورة)

(mp3.موسيقى) (avi.فيديو) (exe.برنامج)

وتتعدّد البرامج الّتي تضطلع بمعالجة هذه الملفّات على الحاسوب، بتعدّد هذه الملفّات وتنوعها ومن هذه البرامج برنامج معالجة النُّصوص (Word) الّذي يقوم بتشغيل الملفّات ذات الامتداد (docx.) وبرنامج (Excel) المتخصِّص في عمل الجداول الممتدّة ذات الطّابع الرّياضي، والّذي يعمل على تشغيل الملفات ذات الامتداد (xlsx.) وبرنامج العروض التّقديميّة (PowerPoint) الذي يعمل على تشغيل الملفّات ذات الامتداد (ppt, .odp.) وبرنامج (La visionneuse de photos Windows) الذي يعمل على فتح ملفات الصّور ذات الامتداد jpg, .gif, .bmp,. tif, .tga.) (pbm, .pgm, .pcx, .png, .ppm.) وبرنامج (Media Player) و(vlc media player) الّذي يعملان على تشغيل ملفات الموسيقى والفيديو ذات الامتداد (mov, .avi, .flv, .mp3, .mp4.) وغيرها من البرامج الإلكترونية التي تضطلع بمعالجة مختلف الملفات الإلكترونيّة.

ثانيا- أجهزة تخزين الملفّات الإلكترونيّة: هي الوسائط الّتي تُدوَّن عليها معلومات الملفّات، بغرض تخزينها وحفظها ومن ثم استرجاعها عند الحاجة إليها؛ باعتبار أنّ هذه الأجهزة تؤمِّن مساحات للتّخزين الإلكترونيّ، وخدمات النّقل

المعلوماتيّ، والنّسخ الاحتياطيّ، الّتي كان يُعتمَد في تأمينها على الورق والأشرطة ما يكلِّف غاليا وجهدا أكبر ووقتا أطول. "فعند ما أصبحت المستودعات الورقية غير قادرة على تلبية احتياجات الإنسان المعرفيّة، خصوصا في جوانب الحفظ والعرض، فتش العقل البشري عن البديل فجاءت تكنولوجيا المعلومات التي اعتبرها العلماء الثورة الصناعيّة الثّانية، التي كانت من أهم مميزاتها؛ اختصار المكان والزمان والجهد والكلفة في عملية الحصول على المعلومات."[2] وتنقسم أجهزة التّخزين إلى أجهزة تخزين داخليّة أو رئيسة وأجهزة تخزين خارجيّة أو ثانويّة، حيث يمثل فيها القرص الصلب الداخلي وحدة تخزين داخلية أو رئيسة، في حين يمثل كل من القرص الصلب الخارجي، والقرص المرن، والقرص المضغوط، والقرص الضوئي، وبطاقة الذاكرة وحدات/ أجهزة تخزين خارجية أو ثانويّة. ويُميّز بين كلّ منها من حيث وظيفته كتثبيت البرامج وأخذ النّسخ الاحتياطيّة، ومن حيث سِعَةِ تخزين المعلومات أو حجم الملفّات التي يمكن أنْ يحتويها، وفي ما يلي عرض هذه الأجهزة الخاصة بخدمات التّخزين والنّقل المعلوماتيّ والنّسخ الاحتياطيّ:

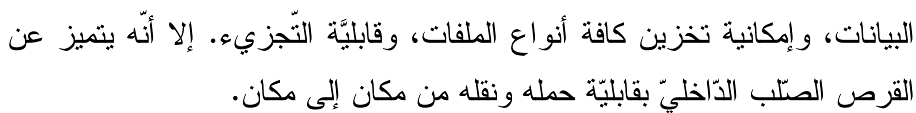


1- القرص الصّلب الدّاخلي (disque dur interne): يُعدُّ القرص الصلب الدّاخليّ وحدة التخزين الرّئيسيّة في الحاسوب، وهو يستخدم لحفظ البيانات داخل الجهاز، ويتكون من أقراص ممغنطة تدور، ويقوم لاقط كهرومغناطيسي بالقراءة والكتابة من وإلى السطح الممغنط. ومن أهم الخصائص الّتي يميّز بها كلّ نوع من الأقراص الصّلبة عن آخر، هو سعة التّخزين وسرعة نقل البيانات. ومن خصائص الأقراص الصّلبة أنّها تتميّز بـــ[3]:

- إمكانية تخزين هائلة، تصل إلى 500 جيـــگا بايت (GB)؛
- سرعة نقل البيانات؛

- إمكانية تخزين كافة أنواع الملفات؛
- إمكانية الوصول المباشر إلى المعلومات؛
- قابليّة التّجزيئ.

2- القرص الصّلب الخارجيّ (disque dur externe): هو عبارة عن وحدة تخزين خارجيّة يتم وصلها بالحاسوب عن طريق منافذ النّاقل التّسلسلي العالميّ (USB) وهو يحمل نفس خصائص القرص الصّلب الدّاخليّ؛ من حيث سعة التّخزين الّتي تصل إلى 1000 جيــگا بايت (GB)/ 1 تيرا بايت (1TB) وكذا سرعة نقل البيانات، وإمكانية تخزين كافة أنواع الملفات، وقابليَّة التّجزيء. إلا أنّه يتميز عن القرص الصّلب الدّاخليّ بقابليّة حمله ونقله من مكان إلى مكان.



3- القرص المرن (disquette): هو عبارة عن أسطوانة دائريّة رفيعة مرنة مصنوعة من مادة مغناطيسيّة، محفوظة ضمن حافظة بلاستيكية مربعة للحماية[4]. وهو وسيلة تخزين قديمة -وهي الآن شبه معدومة- استخدمت لتخزين البيانات والبرامج بين فترة السّبعينات والتّسعينات. ومن خصائص هذا النّوع من أجهزة التخزين أنّه[5]:



- محدود السِّعة؛ حيث تتراوح سعته التّخزينيّة ما بين 1,44 إلى 3 ميــگــا بايت (MB).
- صغير الحجم خفيف الوزن رخيص الثّمن؛
- يُستخدَم أكثر من مرّة في حفظ البيانات وتبادلها؛
- وسيلة غير عمليّة وتتعرّض للتّلف بسرعة، تستخدم غالبا لتخزين الملفات البسيطة.

4- الأقراص المضغوطة (CD\DVD): هي أقراص مصنوعة من مادة بلاستيكيّة ومغطاة بطبقة من الألمنيوم، تعمل بواسطة أشعة اللّيزر لتسجيل المعلومات أو قراءتها، لها قدرة هائلة على تخزين المعلومات، وهو ما تتميز به عن الأقراص المرنة. ويفترق القرص المضغوط (CD) عن قرص الفيديو الرّقمي (DVD) في سعة التّخزين حيث إنّ



(CD) محدود الحجم بـــ 700 ميـــگـــا بايت (MB) بينما (DVD) محدود بـــ 4,7 ميـــگـــا بايت (MB) وفيه نوع آخر محدود 8,5 ميـــگـــا بايت (MB) ومن خصائصهما أنّهما:

- مثاليان لحفظ النّسخ الاحتياطيّة؛
- مثاليان لنَسْخِ البرامج والألعاب والموسيقى والأفلام؛
- مثاليان لنَسْخِ البرامج الإلكترونيّة التّجاريّة.

5- القرص الضّوئيّ (flash disque):

هو عبارة عن جهاز صغير محمول، يتمّ وصله بالحاسوب عن طريق منافذ النّاقل التّسلسليّ العالميّ (USB) تماما مثل القرص الصّلب الخارجيّ. ويأتي هذا النوع من



أجهزة التخزين بأحجام وأشكال مختلفة ومن خصائص الأقراص الضوئيّة أنّها[6]:

- صغيرة الحجم، محمولة، خفيفة الوزن، رخيصة الثّمن، سهلة الاستخدام؛
- مثاليّة لحفظ الملفّات بمختلف أنواعها ونقلها من جهاز إلى جهاز؛
- ذات سعة تخزين عالية؛ ومتوفّرة بأحجام مختلفة سعتها 2 و4 و8 و16 و64 ميـــگـــا بايت (MB)؛
- تسهّل عمليّة نقل المعلومات من حاسوب إلى آخر؛

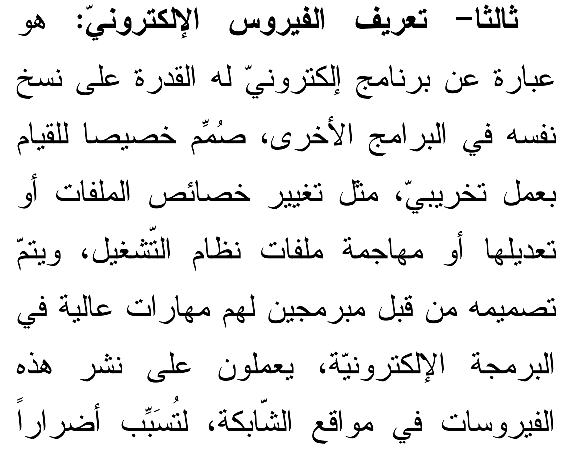
- مثاليّة لتخزين المعلومات بصورة دائمة؛
- تمتاز بالموثوقيّة في حفظ الملفّات ونقلها؛ كما أنّها عمليّة باعتبارها تَخدُم فترة طويلة.

6- بطاقة الذّاكرة (carte mémoire): هي عبارة عن وسيط تخزين أصغر حجما من القرص الضّوئيّ، يتمُّ وصلها بالحاسوب عبر منفذ قارئ بطاقة الذَّاكرة وكذا منفذ النّاقل التّسلسليّ العالميّ (USB). وتُعدُّ بطاقة الذّاكرة أحدث وسائط التّخزين وقد زادت سعتها، وصغر حجمها، وانخفض سعرها باستمرار؛ ممّا أدّى إلى انتشارها مقارنة بوسائط التّخزين الأخرى. وتمتاز بطاقات الذاكرة بما يلي[7]:



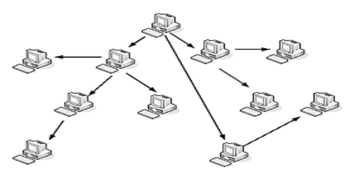
- صغر حجمها ومناسبة ثمنها؛
- سعتها التخزينيّة الكبيرة؛
- سهولة حملها؛
- قدرتها على التّحمل.





ثالثا- تعريف الفيروس الإلكترونيّ: هو عبارة عن برنامج إلكترونيّ له القدرة على نسخ نفسه في البرامج الأخرى، صُمِّم خصيصا للقيام بعمل تخريبيّ، مثل تغيير خصائص الملفات أو تعديلها أو مهاجمة ملفات نظام التّشغيل، ويتمّ تصميمه من قبل مبرمجين لهم مهارات عالية في البرمجة الإلكترونيّة، يعملون على نشر هذه الفيروسات في مواقع الشّابكة، لتُسَبِّب أضراراً





وخسائر تتراوح في حجمها من تدمير ملفّ صغير إلى تدمير بيانات تُقدَّر بأثمان باهظة[8]. وتُبرمَج في العادة معظم الفيروسات على شكل ملفّ تطبيق (exe.) وعند تحميلها على الحاسوب من مواقع الشَّابكة، تنشط بمجرد فتح الملفّ الّذي تمّ تحميله مرفقا بالفيروسات. ويُقدَّر عدد الفيروسات المستجدة كُلَّ يوم على مواقع الشّابكة ما بين 10–20 فيروساً جديداً.

1– مصدر الفيروسات: لا تتعدَّد مصادر الفيروسات بتعدد طبيعتها، بل –على اختلافها– مصدرها واحد، هو الشّابكة (الإنترنيت) الّتي يتم تصفّح مواقعها وتحميل الملفاتّ الإلكترونيّة منها، ما يسمح للفيروسات بالانتقال إلى الحاسوب وأجهزة التّخزين، رُفقَة الملفّات الّتي يتمّ تحميلها. وتنتقل الفيروسات إلى غيرها من الملفَّات الّتي تمّ تخزينها في هذين الجهازين، كما تنتقل إلى غيرها من الحواسيب وأجهزة التخزين عن طريق وصلها مباشرة بالجهاز المصاب بالفيروسات؛ وهذا بفضل خاصيّة النّسخ التي تتمتّع بها الفيروسات، والّتي تسمح لها بالانتشار.

2– خصائص الفيروسات الإلكترونيّة: تتميّز الفيروسات باعتبارها برامج إلكترونيّة، عن بقيّة برامج الحاسوب بأربعة خصائص، تسمح لها بالقيام بدورها الّذي صُمِّمَت لأجله، وهي: **خاصيّة التّناسخ** التي تسمح لها بالانتشار لإصابة أكثر عدد من الحواسيب والملفّات الإلكترونيّة، **وخاصيّة التّخفي والتّمويه** عن طريق الارتباط ببرامج أخرى؛ لخداع المستخدمين في الانتقال إلى الحواسيب وأجهزة التّخزين، و**خاصيّة الاختراق** الّتي تؤمِّن لها الانتقال من موقع إلكترونيّ إلى آخر و**خاصيّة التّدمير** الّتي تسمح لها بتخريب البرامج والملفّات الإلكترونيّة، وهي على النّحو الآتي[9]:

2–1 التّناسخ: هي خاصّية تسمح للفيروسات بالانتشار لإصابة أكثر عدد من الأجهزة الإلكترونيّة وتتمّ عن طريق وسائل الاتّصال بين الحواسيب، وأجهزة التّخزين، وقابلية الفيروسات على نسخ نفسها وضعف برامج الحماية في تلك الأجهزة.

2-2 التّخفي: هي خاصيّة تسمح للفيروسات بخداع المستخدمين في عملية دخولها إلى الحاسوب عن طريق الارتباط ببرامج أخرى والتّمويه والتشبّه؛ حيث ترتبط الفيروسات ببرامج تقوم بأعمال لطيفة أو لها قدرة عرض أشياء مثيرة وعند بداية تشغيلها تدخل إلى النّظام وتعمل على تخريبه، دون ملاحظة وجوده عن طريق عرض ملفّات البرنامج. ومن الفيروسات ما تقوم بالتخفي في أماكن خاصة مثل ساعة الحاسوب وتنتظر وقت التنفيذ، كما أنّ منها ما يقوم بإخفاء أي أثر له؛ لدرجة عدم عجز مضادات الفيروسات وعن كشفها وملاحظة وجودها، ثم تقوم بنسخ نفسها إلى البرامج بخفة وسريّة.

3-2 الاختراق: هي خاصية تتمكّن من خلالها الفيروسات من اختراق أكبر عدد من المواقع التي يمكن للمستخدم أنْ يتصفّحها أو يقوم بتحميل الملفّات منها.

4-2 التّدمير: هي خاصيّة تتمكَّن من خلالها الفيروسات من القضاء على خصائص البرامج أو الملفّات الإلكترونيّة ما يجعلها عرضة للتلفّ، وتتعدّى أضرار الفيروسات من خلال هذه الخاصيّة إتلاف الملفّات والبرامج الإلكترونيّة إلى تعطيل الأجهزة الدّاخليّة للحواسيب كالقرص الصلب أو معالج المعلومات (processeur).



ويشبه تأثير الفيروسات الإلكترونيّة على الحواسيب وأجهزة التخزين والملفات الإلكترونية إلى حد كبير تأثير الفيروسات العضوية على الجسم وأعضائه وتنقلها

من شخص لآخر، ولهذا سمِّي الفيروس الإلكترونيّ بهذا الاسم، ويوضّح الجدول التّالي الصّفات المشتركة بين الفيروس العضويّ والفيروس الإلكترونيّ[10]:

الفيروس العضويّ	الفيروس الإلكترونيّ
يقوم الفيروس العضوي بتغيير الخصائص العضوية لخلايا الجسم	يقوم فيروس الحاسوب بتغيير خصائص الملفات ووظائف البرامج الإلكترونيّة الأخرى
يتكاثر الفيروس العضوي ويتسبب في إنشاء فيروسات جديدة	يقوم فيروس الحاسوب بإعادة إنشاء نفسه فيظهر وكأنه يتكاثر ذاتيا
الخلية التي تصاب بالفيروس العضوي لا تصاب بالفيروس نفسه مرة أخرى	إذا أصاب فيروس الحاسوب الآلي برنامجا معينا فلا يصيبه مرة أخرى
الجسم الذي ينقل إليه الفيروس العضوي العدوى، قد يبقى مدة طويلة دون ظهور أعراض المرض عليه	البرامج المصابة بفيروس الحاسوب قد تبقى مدة طويلة دون ظهور أعراض تخريبيّة عليها
في بعض الحالات يقوم الفيروس العضوي بتغيير شكله	كذلك بعض فيروسات الحاسوب لديها القدرة على تغيير شكلها حتى يصعب اكتشافها والتغلب عليها
تنتقل الفيروسات العضوية من شخص إلى آخر	لدى الفيروسات قدرة الانتقال من جهاز حاسب إلى آخر
الفيروس العضويّ ليس كائنا حي ولكنه جزء من الحمض النووي داخل غلاف وقائي، وليؤثر في جسم الإنسان لا بد أن يحقن	فيروس الحاسوب لا يعمل بمفرده، بل يلزمه التعلق والالتصاق على برنامج آخر، ومتى ما تعلق به وتمّ تشغيل البرنامج فإنه ينتشر في برامج أخرى

حمضه النووي داخل خلية حتى تمتلئ بالحمض النووي، وبالتالي تنفجر وتطلق الفيروس أو أنّ يتقوقع خارجها ويتركها حيّة	ليلتصق بها ويلوثها

3- أنواع الفيروسات: تتعدَّد طبيعة الفيروسات بتعدُّد مهمّتها الّتي صُمّمت لأجلها؛ فمنها الّتي تستهدف تدمير البيانات والملفَّات المخزّنة في الحاسوب، ومنها الّتي تستهدف إتلاف نظام الحاسوب (Windows) ومنها الّتي تستهدف أداء الحواسيب والشَّبكات، ما يؤثّر على سرعة معالجة الحاسوب تؤثّر على. وهي بذلك تأخذ أشكالا عديدة في القيام بمهمتها التخريبية منها[11]:

3-1 حصان طروادة (Trojan Horse): هو برنامج صُمِّم لجمع المعلومات والبيانات الشّخصيّة الخاصة بالمستخدمين مثل: اسم المستخدم، وكلمة السِّر، ونقلها إلى الطرف الآخر؛ لاستعمالها في دخول الحسابات والمواقع والحواسيب الخاصّة والتّحكم بالملفّات تحكُّما كاملا. وتختلف فيروسات أحصنة طروادة عن الفيروسات العادية، في كونها لا تعيد إنتاج نفسها (عدم التّناسخ) بل تعتمد الشَّبكة في دخولها إلى الحواسيب.

وسُمِّي فيروس حصان طروادة بهذا الاسم نسبة إلى حصان الأسطورة الإغريقية الواردة في ملحمة الأوديسا لهوميروس، حيث ترك الجيش الإغريقي بعد أن تظاهر بإنهاء الحصار الطويل على مدينة طروادة، حصانا خشبيا ضخما هدية لسكان طروادة، وكان يختبئ ضمنه مجموعة من الجنود الإغريقيين الأشداء، وعند ما رحل الجيش وأدخل السكان الحصان إلى داخل أسوار المدينة، خرج الجنود منه وانقضوا على الحامية، وسقطت المدينة في أيدي الإغريق. وتعتمد فيروسات أحصنة طروادة المبدأ نفسه، فهي تتنكّر في شكل دعابات برمجية، أو موسيقى أو مقاطع فيديو أو عروض، أو برامج يبدو مظهرها حسنا وملائما، وعند ما يحمل المستخدم واحدا من هذه البرامج، تنتقل أحصنة طروادة إلى حاسوبه آليا.

3-2 فيروسات الدِّيدان (Worms): هي عبارة عن برامج إلكترونيّة تنتقل تلقائيًّا من مواقع الشّابكة إلى الحواسيب، تمتاز بسرعة الانتشار والقدرة على إنتاج نفسها بنسخ نفسها عن طريق الشَّابكة عدّة مرّات دون الحاجة إلى وسيطٍ برمجيّ وهي تستهدف استهلاك موارد الشّبكة في الحواسيب لإبطاء قوة تدفُّق الشّابكة إليها.

3-3 القنابل المنطقيّة (Iogic Bomb): هي برامج إلكترونيّة تمّ تصميمها لتخريب بعض البرامج ومسح بعض بيانات الملفّات الخاصّة، يرتبط نشاطها بحدوث تطبيق معيّن على الحاسوب يضعه مبرمجها شرطا لتنشيطها، كحذف اسم واضع فيروس القنبلة من كشوف الرّواتب الّذي قد يؤدي إلى حذف البيانات كلّها ولهذا سُمِّي هذا النّوع من الفيروسات القنابل المنطقيَّةُ.

3-4 القنابل الموقوتة (Time Bomb): هي برامج إلكترونيّة تمّ تصميمها لتخريب أو مسح الملفّات الخاصّة من الحاسوب، يرتبط نشاطها بوقت محدّد اعتمادا على ساعة الحاسوب، كتصميم قنبلة موقوتة لمسح كافّة الملفّات ذات الامتداد (docx.ملف) من القرص الصّلب في رأس السّنة الميلادية مثلا. ولهذا سمّي هذا النّوع من الفيروسات القنابل الموقوتة.

3-5 فيروسات العتاد (Hardware Viruses): هي برامج إلكترونيّة تُصمَّم للقيام بتنفيذ ملايين العمليّات الحسابيّة المتواليّة؛ بدون استخدام أوامر للإخراج أو الإدخال، وهو ما يلقي عبئا كبيرا على وحدة المعالجة المركزيّة (processeur)؛ مما يؤدِّي إلى ارتفاع درجة حرارتها وثمّ احتراقها.

4- مهدِّدات الفيروسات: تتعدَّى مخاطر الفيروسات وتهديداتها جهاز الحاسوب وأجهزة التّخزين إلى الملفات الإلكترونيّة، ومن الأضرار التي قد تلحقها الفيروسات **بالحواسيب وأجهزة التّخزين**، ما يلي[12]:

- استهلاك مساحات تخزين عالية واستغلال جزء كبير من ذاكرة الحاسوب؛
- استهلاك حيّز من طاقة المعالجة، ما يقلل من سرعة الحاسوب في معالجة الملفات؛

- استهلاك برمجيات كشف الفيروسات؛ مما يشكِّل عبئاً على المستخدم والجهاز والتّكلفة؛

- تعطيل نظام تشغيل الحاسوب أو جهاز التّخزين.

أما الأضرار التي قد تلحقها الفيروسات **بالملفّات الإلكترونيّة**، فتتمثّل في ما يلي:

- التّعدي على حقوق الملكيّة الفكريّة بالتّعديل في الملفات دون موافقة مالكيها؛
- فقدان الملف أحد خصائصه كخاصّية القراءة وخاصّية العرض؛
- تغيير أيقونة الملفّ لتضليل المستخدم؛
- نسخ عدّة نسخ افتراضيّة للملف بصيغة اختصار لتضليل المستخدم؛
- إتلاف الملفّ الإلكترونيّ نهائيًّا.

5- أعراض الفيروسات: تظهر على الحواسيب والبرامج المثبَّتة عليها والملفَّات المخزّنة فيها، في حالة إصابتها بالفيروسات، عدّةُ أعراض تشير إلى إصابتها بأحد أنواع الفيروسات، مثلها مثل الأعراض الّتي قد تظهر على المريض المصاب بأحد الفيروسات العضويّة، ومن هذه الأعراض الّتي قد تظهر على الحواسيب أو الملفات أو البرامج الإلكترونيّة ما يلي[13]:

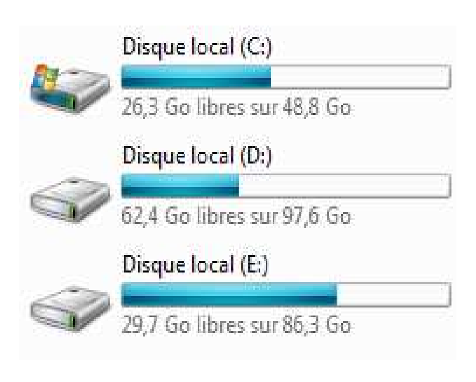
- بُطءٌ في أداء الحاسوب؛
- انخفاض سعة الذّاكرة الرّئيسة بشكل مفاجئ؛
- انخفاض سعة القرص الصلب بشكل واضح؛ بسبب تناسخ الفيروسات، ما يؤدّي إلى تباطؤ في قراءته؛
- تغير شكل إيقونات بعض الملفَّات؛
- تضخم حجم بعض الملفَّات وذلك بسبب اختفاء الفيروسات ضمنها.
- ظهور رسائل خطأ غير اعتيادية؛
- حدوث خلل في أداء لوحة المفاتيح كظهور أحرف غريبة أو خاطئة عند النقر على حرف معين؛

- سماع نغمات موسيقية غير مألوفة من مكبر الصوت في جهاز الحاسوب؛
- توقّف النّظام بلا سبب؛
- توقف بعض البرامج عن العمل؛
- إنشاء ملفّات عشوائية بدون تدخل من المستخدم؛
- تلف بيانات الملفّات؛
- تغيير اسم القرص؛
- إجهاد الأجزاء الميكانيكيّة للحاسوب.

وهذه الأعراض مجتمعة منها ما يظهر على الحاسوب ومنها ما يظهر على برامج التطبيق، ومنها ما يظهر على الملفات الإلكترونيّة الخاصّة.

رابعا- تقنيات التّعايش الإلكترونيّ مع الفيروسات: لا نقصد بالتّعايش الإلكترونيّ مع الفيروسات ترك المستخدم للحاسوب ملفاته الإلكترونيّة تحت تهديد هذه الفيروسات؛ بل نقصد به مصطلحًا ومفهومًا **تأمين الملفات الإلكترونيّة وحمايتها في ظلّ تهديدات هذه الفيروسات وتجدّدها، وعدم كفاءة بعض مضاداتها في إزالة تهديدها.** وبخاصّة مع عدم التَّحكم التّامّ لغير المتخصّصين في هذه التّقنيّة في تخزين المعلومات ونقلها من جهاز إلى آخر. ويتمّ هذا التّعايش بمعرفة المستخدم هذه التّقنيّة طبيعةَ الفيروس المهدّد لحاسوبه وملفاته، وإدراك مدى خطورته على الحاسوب وأجهزة التخزين والملفات معا ومعرفة برامج إزالة تهديده واستعادة ملفّاته، في حال تعرُّضها للفيروسات؛ حتى يتمكّن من تأمين هذه الملفات ومعالجتها على الحاسوب أو تخزينها أو نقلها بشكل آمن. ويتمّ تأمين هذه الملفات في ظلّ تهديدات هذه الفيروسات وتجدُّدها من خلال التِّقنيات الآتية:

1- حفظ الملفّات في الأجزاء الأقل عرضة للفيروسات في القرص الصّلب الدّاخليّ: تُعدُّ الأجزاءُ الأقلُّ عرضة للفيروسات في القرص الصّلب الدّاخليّ الخاصّ بتخزين الملفَّات في الحاسوب، الجزء (D) و(E) من القرص باعتبار أن الجزء (C) الخاص بنظام التّشغيل، يكون على اتصال مباشر بالشّابكة ما يجعله أكثر عرضة للفيروسات وإتلاف الملَفَّات.

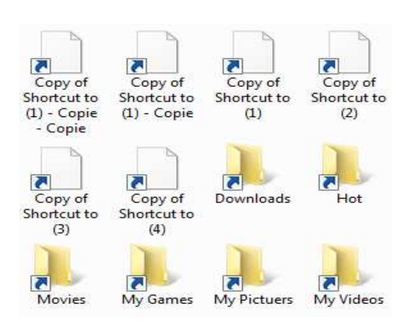


2- تثبيت مضادات الفيروسات على الحاسوب، وتحديثها دوريًّا: تصمّم برامج مضادات الفيروسات خصّيصا؛ لمحاربة الفيروسات التي يتم التقاطها على جميع مواقع الشّابكة وأجهزة التخزين المعلوماتيّ، من خلال تزويدها بآليات التّعرف على الفيروسات، وإزالتها نهائيًّا من الحاسوب المتّصل بالشّابكة، إلاّ أنّه لمّا كان مبرمجو الفيروسات يبتكرون في كلّ مرَّة صيغا جديدة للفيروس، فإنّه يتعذر على مضاداتها التّعرف عليها إلا من خلال التحديث المستمر لها؛ حتَّى يتسنى لها معرفة أنواع الفيروسات المستجدة على مواقع الشّابكة ومحاربتها؛ لإزالة تهديدها على الحاسوب والملفَّات معا، ويستلزم التَّحديث المستمرّ لمضاد الفيروسات، وضعه تحت خدمة التّحديث الآلي، ليتمكّن من التقاط ما استجد من فيروسات على مواقع الشّابكة. "ومن البرامج الفعَّالة في عالم مضادات الفيروسات (Kaspersky Antivirus) و(Avast Antivirus) و(AVG Antivirus) و(Microsoft Security) و(Bitdefender Antivirus)"[14].



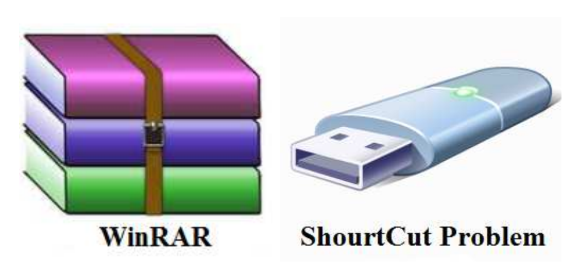








3- تثبيت برامج استعادة خصائص الملفَّات: تعجز مضادات الفيروسات أحيانا بعد فحص موقع الشّابكة الّذي يتَّصل به المستخدم، أو الحاسوب أو جهاز التّخزين عن التقاط الفيروسات المستجدة في مواقع الشابكة، ما يجعل أجهزة التّخزين والملفَّات عرضة للإصابة بالفيروسات. ومن أعراض إصابة الملفات بهذه الفيروسات، هو ظهور الملفات على شكل اختصار مكتب (Raccourci) أو فقدان الملفّ تماما من جهاز التّخزين؛ بسبب تخلّص الفيروس من خاصيّة الامتداد والعرض (Affichage) اللّتيْن تتميّز بهما الملفات الإلكترونيّة. ويستدعي في هذه الحالة تأمين الملفات المفقودة واستعادة خصائصها تثبيت البرامج الخاصّة باستعادة خصائص الملفَّات، ومن بين هذه البرامج برنامج إظهار الملفَّات (visible) وبرنامج حلّ مشكلة الاختصار (ShourtCut Problem) وبرنامج فك الملفَّات المضغوطة (WinRAR). وهي البرامج التي تسمح بتأمين الملفَّات التي تعرضتّ إلى إصابة الفيروسات، من خلال استعادتها خاصيتي الامتداد والعرض اللّتين تفقدهما الملفات الإلكترونيّة بسبب إصابتها بالفيروسات.





ويشتغل كلّ من برنامج حلّ مشكلة الاختصار (ShourtCut Problem) وبرنامج فك الملفَّات المضغوطة (WinRAR) في تأمين الملفّات المفقودة على جهاز التّخزين، واستعادة خصائص الملفات المصابة بالفيروسات، بعد تثبيتهما على الحاسوب، ثمّ فتح جهاز التّخزين المصاب بالفيروسات بواسطة أحد هذين البرنامجين، في حين يشتغل برنامج إظهار الملفّات (visible) بتثبيته مباشرة على جهاز التّخزين المصاب بالفيروسات، وانتظاره مدة كافية لقراءة جميع الملفات المخزنة على الجهاز واستعادة الملفّات المخفيّة.

خاتمة: تُعَدُّ هذه التِّقنيات التي تعرضنا إليها في بحثنا هذا، الطريقة المثلى لتأمين الملفَّات الإلكترونيّة في ظلّ تهديدات الفيروسات المستجدة في عالم الشابكة، وتحقيق التّعايش الإلكتروني مع هذه الفيروسات باعتبارها أحد مهدِّدات الأمن المعلوماتي وتأمين خدمات التّخزين والنّقل والنّسخ التي توفِّرها أجهزة التّخزين المعلوماتي والحفظ الاحتياطيّ. وهذه التّقنيات التي ذكرناها أقل جهدا وتكلفة في حال اتخاذها سبيلا لتأمين الملفات والتّخلص من مهددات الفيروسات. وقد أمّنت خدمات تعريب البرمجيات تعريب برمجية كل من هذه التّقنيات، ما يتيح لمستخدمي الحاسوب في الوطن العربي التعامل معها بسهولةٍ وفهمٍ جيّدٍ، في تثبيتها واستخدام تطبيقاتها.

الهوامش

1- ينظر: ويكيبيديا الموسوعة الحرّة "ملف حاسوب" تم استرجاعه يوم: 09-10-2015، على الرابط [https://ar.wikipedia.org/wiki].

2- فريا، "وسائط التخزين" تم استرجاعه يوم: 09-10-2015، على الرّابط
[http://storagemedium.blogspot.com].

3- ناصر الكناني "الذاكرات وأنواعها وحدات التخزين الثانوية" تم استرجاعه يوم: 12-10-2015، على الرابط:
[http://www.aukran.com/showthread.php?t=7921].

4- ينظر: ناصر الكناني "الذّاكرات وأنواعها وحدات التّخزين الثَّانويَّة" تمّ استرجاعه يوم: 20-10-2015، على الرّابط
[http://www.aukran.com/showthread.php?t=7921].

5- فريا "وسائط التّخزين" تم استرجاعه يوم: 09-10-2015، على الرّابط
[http://storagemedium.blogspot.com].

6- ينظر: فريا "وسائط التّخزين" تم استرجاعه يوم: 09-10-2015، على الرّابط
[http://storagemedium.blogspot.com].

7- ناصر الكناني "الذاكرات وأنواعها وحدات التخزين الثّانوية" تم استرجاعه يوم: 12-10-2015، على الرابط:
[http://www.aukran.com/showthread.php?t=7921].

8- ينظر "تعريف الحاسب الآليّ" تم استرجاعه يوم: 16-10-2015، على الرابط
[http://faculty.ksu.edu.sa/jaffer/fun/].

9- ينظر: خالد علي المرحبيّ "الفيروسات" تمّ تحميله يوم: 10-10-2015، على الرّابط
[http://www.noor-alyaqeen.com/up//uploads/files/domain-92612890f6.doc].

10- خالد علي المرحبيّ "الفيروسات" تمّ تحميله يوم: 10-10-2015، على الرّابط
[http://www.noor-alyaqeen.com/up//uploads/files/domain-92612890f6.doc].

11- ينظر: خالد علي المرحبيّ "الفيروسات" تمّ تحميله يوم: 10-10-2015، على الرّابط

http://www.noor-alyaqeen.com/up//uploads/files/domain-]
.[92612890f6.doc

12- ينظر: ربى شتشاوي "تعريف الفيروسات" تم استرجاعه يوم، 09-10-2015 على الرّابط: [http://mawdoo3.com].

13- خالد علي المرحبيّ "الفيروسات" تمّ تحميله يوم: 10-10-2015، على الرّابط
http://www.noor-alyaqeen.com/up//uploads/files/domain-]
.[92612890f6.doc

14- ينظر "أفضل 5 برامج مضادة للفيروسات في نظامي Windows 8 و8.1!!" تم استرجاعه يوم 15-10-2015 على الرّابط

[http://www.freedomssl.com/2014/11/5-windows-8-81.html].

الإطار القانوني لأمن المعلومات

أ.نجيبة بادي بوقميجة

جامعة الجزائر 1 –كلية الحقوق –

مقدمة : تعتبر المحافظة على المعلومات بشكل دائم أمرا صعبا، خاصة في هذا العصر الذي تستخدم فيه التقنيات الحديثة كأدوات للتجسس الصناعي، وتنتشر فيه القرصنة دوليا وداخليا، فهناك أعداد متزايدة من الشركات –حتى الشركات ذات السمعة الدولية–قامت بتبني نظام التجسس الاقتصادي لهدر أمن المعلومات.

وهذه المشكلة ليست مقصورة على الشركات فقط بل تمتد إلى الدول أيضا وتتورط فيها، فقد أعلنت المباحث الفيدرالية الأمريكية أن هناك أكثر من ثلاث وعشرين حكومة تشمل: الحكومة الفرنسية، اليابانية، الألمانية، السويسرية السويدية، الروسية، قد تورطت بالفعل في محاولة الاستيلاء على معلومات اقتصادية مهمة خاصة بالولايات المتحدة الأمريكية. وهذا التجسس يتركز بمعدل أكبر في المناطق ذات التركيز التكنولوجي والبحثي والأنشطة التطويرية مثل وادى السليكون في الولايات المتحدة الأمريكية –وهو الأكثر استهدافا – ونورث كارولينا ودالاس وبوسطن وواشنطن ونيوجرسي حيث تتمركز شركات الأدوية والتكنولوجيا وصناعة الإلكترونيات والفضائيات والتكنولوجيا الحيوية، ففي وادى السليكون وحده أكثر من عشرين وكالة تتبع المباحث الفدرالية FBI تنفق كل وقتها في تحريات أو تحقيقات سرقات الأسرار التجارية، وليست التكنولوجيا المتقدمة هي المستهدفة فقط ولكن أيضا المعلومات السرية التجارية مثل: خطط التسويق والملفات الشخصية وتكلفة التصنيع وقائمة العملاء والمنتجات ومعلومات التطوير والتسعير

والمبيعات. وبخصوص المعلومات السرية أو ما يعرف بالأسرار التجارية فإنه لا يوجد تعريف على المستوى العالمي بخصوصها، لأن التعريف يختلف باختلاف

التشريعات الخاصة في هذا المجال، حيث تتعدد الحماية على المستوى الوطني والدولي.

الأمر الذي يؤدي بنا إلى طرح الإشكالية المتعلقة بأفضل حماية قانونية يمكن توفيرها للمحافظة على أمن المعلومات.

والإجابة عن الإشكالية تكون وفق الخطة التالية:

I / الحماية الدولية للمحافظة على أمن المعلومات.

II /الحماية الوطنية للمحافظة على أمن المعلومات.

I – الحماية الدولية :

فأما على المستوى الدولي نجد اتفاق جوانب حقوق الملكية الفكرية المتصلة بالتجارة، وهو الاتفاق الذي تديره المنظمة العالمية للتجارة، والذي يصطلح عليه باتفاق "تربس"، وهو أول اتفاق دولي ينص على إدراج الحماية ضد التجسس الاقتصادي والصناعي ضمن حقوق الملكية الفكرية، واصطلح عليها بـــ"المعلومات غير المفصح عنها" في جولة أورجواي، رغم اعتراض الدول النامية على إجراء المفاوضات في إطار الجات ومناداتها بأن تعقد مفاوضات الملكية الفكرية تحت إشراف المنظمة العالمية للملكية الفكرية[1].

وقد اعترض ممثلو العديد من الدول مثل: الهند، البيرو، والبرازيل على حماية الأسرار التجارية عن طريق قواعد الملكية الفكرية، باعتبار أن "الإفصاح"، وهو المقابل الذي يحصل عليه المجتمع في نظير الاعتراف بحقوق المخترع الإستئثارية لا وجود له في أسرار التجارة.

ومن المسائل التي قوبلت باعتراض من جانب ممثلي الدول المشاركة في الاجتماع ما تضمنه الاقتراح الأمريكي من أحكام تتعلق بحماية البيانات أو المعلومات التي تقدم إلى الجهات الحكومية [2].

ووفقا لهذا الاقتراح فإن حصول شخص من الغير على أسرار التجارة دون علمه بأن الإفصاح عنها أو استعمالها غير مصرح به من قبل مالكها أو حائزها الشرعي يعد اعتداء على حقوقه التجارية من قبل الغير على الرغم من حسن نيته.

وقد تحفظ عدد كبير من ممثلي الدول على هذا الاقتراح، وأبدوا اعتراضهم على هذا التوسع وقد طرحت خلال المناقشات عدة بدائل لحماية الأسرار التجارية عن طريق قواعد قمع المنافسة غير المشروعة والقانون الجنائي وقانون العقود وقانون العمل.

ثم نوقشت مواد المشروع من الدول الأطراف وأدخلت عدة تعديلات عليه، ثم أعد مشروع آخر شمل هذه التعديلات للعرض على المؤتمر الوزاري لوزراء الدول الأطراف في الجات المنعقد في بروكسل في ديسمبر 1990.

وقد استمرت المفاوضات عدة سنوات غير أن الوثيقة الوحيدة الهامة التي أعدت بعد ذلك هي المشروع النهائي لعام 1991.

وقد اعتمد هذا المشروع على الاقتراحات والصياغات المقدمة من وفود الدول التالية: الاتحاد الأوربي[3]، الولايات المتحدة الأمريكية[4]، الأرجنتين، البرازيل الشيلي، الصين، كولومبيا، كوبا، مصر، الهند، نيجيريا، بيرو، تنزانيا وأورجواي ولحقت بهم بعد ذلك باكستان وزيمبابوي[5]، سويسرا[6]، واليابان[7] وأستراليا[8].

وفي نهاية المطاف، استبعدت المواقف والانتقادات الرامية إلى عدم حماية الأسرار التجارية، ويتضح ذلك جليا من خلال نص المادة الأولى، الفقرة 2 من اتفاقية تريبس الوارد كالآتي:

"في هذه الاتفاقية يشير اصطلاح "الملكية الفكرية" إلى جميع فئات الملكية الفكرية المنصوص عليها في الأقسام من 1 إلى 7 من الجزء الثاني.

وبالرجوع إلى الجزء الثاني والمتعلق بالمعايير المتعلقة بتوفير حقوق الملكية الفكرية ونطاقها واستخدامها، نجده يتفرع إلى ثمانية أجزاء، تتعلق الأجزاء السبعة الأولى بما يلي:

1/ حقوق المؤلف والحقوق المتعلقة بها.

2/ العلامات التجارية

3/ المؤشرات الجغرافية

4/ التصميمات الصناعية

5/ براءات الاختراع.

6/ التصميمات التخطيطية (الرسومات الطبوغرافية) للدوائر المتكاملة.

7/ حماية المعلومات السرية.

والمادة 39 (2) من اتفاقية التربس تطرقت للشروط العامة لحماية المعلومات غير المفصح عنها، وأوجبت توافر شروط معينة في المعلومات حتى يمكن حمايتها قانوناً وهي: السرية، وأن يكون للمعلومات قيمة تجارية نظرا لكونها سرية، وأن يتخذ حائز المعلومات تدابير جدية للمحافظة على سريتها ونستعرض هذه الشروط كل في عنصر مستقل:

الشرط الأول: سرية المعلومات (1).

الشرط الثاني: القيمة التجارية للمعلومات نظرا لسريتها (2).

الشرط الثالث: اتخاذ حائز المعلومات تدابير جدية للمحافظة على السرية (3).

1 / سرية المعلومات: للتعرف هل يمكن اعتبار المعلومة من قبيل أسرار الأعمال نتساءل عن طابعها السري، أو بتعبير آخر البحث عن مدى علم الغير بهذه المعلومة.

فمن وجهة النظر الشخصية ولكي تعتبر المعلومة سرية يجب على المبدع أو المخترع أن تكون له مصلحة معتبرة في الاحتفاظ بالسرية دون أن يترجم ذلك بالضرورة إلى التزامات تعاقدية، وينبغي أن يكون قد عبر عن نيته في احترام الطابع السري للمعلومة، وغالبا ما يشترط وجود إجراءات خاصة قد اتخذت لحماية الأسرار، ولا يكفي أحيانا أن تكون المعلومة قد بلغت تحت خاتم السرية دون أي قيد أو شرط[9].

ومن وجهة النظر الموضوعية، لا يمكن اعتبار المعلومة سرية إلا إذا كانت غير معروفة إلا لدى فئة صغيرة من الأشخاص، أي بعبارة أخرى إذا كانت بصفة عامة غير معروفة من طرف المنافسين وعامة المستهلكين، فانه حتى طلب براءة الاختراع. يمكن اعتباره معلومة سرية في حالة عدم نشره من طرف مصلحة البراءات[10].

فالمعلومات المعروفة لدى الجمهور، أو لطائفه تضم عدداً كبيراً من الأشخاص المتخصصين في مجال نشاط تجارى أو صناعي معين لا تدخل في عداد أسرار التجارة التي يحميها القانون.

ولا يشترط أن تكون درجة السرية التي تتوافر في المعلومات مطلقة، حيث أن المعلومات لا تفقد طابع السرية لمجرد أن عددا محدودا من الأشخاص يعرفونها. فإفشاء صاحب أسرار التجارة لعدد قليل من الأشخاص عن تلك الأسرار (مثل بعض العاملين في المشروع، أو المستشارين، أو المحامين) لا يؤدى إلى انحسار صفة السرية عن المعلومات، طالما يوجد التزام على هؤلاء بكتمان هذه الأسرار وعدم الإفصاح عنها[11].

كما أن السر لا يمكنه أن يكون مطلقا، كون المعلومة يمكن أن تكون قد اكتشفت من طرف الغير بطريقة مستقلة، حيث أنه لمعرفة هل المعلومة السرية يمكن تصنيفها من قبيل أسرار الأعمال القابلة للحماية، يجب أن نتساءل أو نطرح الأسئلة التالية:

- هل هذه المعلومة تتضمن عناصر ليست سرية عند دراستها بانفصال؟.
- هل من الضروري أن يعلم بها العمال لممارسة عملهم على أكمل وجه؟.
- هل هي مخصصة للمسئولين عليها فقط، أم أنها يمكن أن تكون معروفة من قبل العمال الآخرين؟ .

2- وجود قيمة تجارية للمعلومات: وهذا الشرط يعكس الحاجة نحو حماية الاستثمارات التي تخصصها المشروعات للتوصل إلى المعلومات والمعارف الجديدة بما يخدم ويطور الأداء الاقتصادي للمشروع.

ولا يلزم تقدير قيمة المعلومات بدقة للتحقق من توافر هذا الشرط، إذ يكفى أن تكون المعلومات نافعة أو مفيدة في مجال نشاط المشروع، لأن فائدة المعلومات أو مقدار نفعها هي التي تجعل لها قيمة اقتصادية في مجال النشاط. ويعتبر الشرط متحققا إذا كانت المعلومات السرية تعطى لصاحبها ميزة نسبية في مجال نشاطه في مواجهة منافسيه الذين يجهلونها[12].

ويكفى لتحقق شرط وجود قيمة اقتصادية للمعلومات احتمال أن تصبح للمعلومات السرية قيمة اقتصادية في المستقبل، فلا يشترط أن تكون قيمتها حالية.

ولا شك في أن القيمة الاقتصادية للمعلومات ترتبط بالسرية، لأن قيمة المعلومات تنخفض كلما زاد عدد حائزيها، كما ترتبط بمدى صعوبة أو سهولة حصول الغير على المعلومات بوسائله الخاصة. وبمعنى أكثر وضوحا يجب أن تكون المعلومات السرية حصيلة جهود بذلت، أو مبالغ مالية أنفقت للتوصل إليها.

3- اتخاذ حائز المعلومات تدابير جدية للمحافظة على السرية: نظرا إلى طابع المعلومات السرية ذاته فإنه لا يجوز للغير الكشف عنها أو الحصول عليها أو الانتفاع بها دون موافقة مالكها الشرعي. والمالك الشرعي هو الذي يقرر إعطاء المعلومات صفة السرية باتخاذ التدابير المناسبة للحفاظ على سريتها.

وقد يرد شرط عدم الكشف عن المعلومات أو الحصول عليها أو الانتفاع بها دون موافقة مالكها الشرعي مباشرة في عقد أو اتفاق شفهي يبرم مثلا بين المالك الشرعي والموظف لديه، أو بين المالك الشرعي ومورد يتعامل معه في إطار مشروع محدد. وقد ينشأ بصورة غير مباشرة عن الظروف المحيطة بالمعلومات كالتدابير التي يتخذها المالك الشرعي للحفاظ على السرية على نحو يتيح للغير إدراك طابعها السري[13].

حيث يتمتع الموظفون السابقون بالحق في الانتفاع بأي مهارات أو خبرة أو معارف اكتسبوها خلال فترة العمل السابقة في سبيل كسب رزقهم. ولا ريب في أنه يصعب غالبا تمييز الحد الفاصل بين الانتفاع الشرعي بالمهارات والمعارف والخبرة المكتسبة خلال فترة العمل، والكشف غير المشروع عن المعلومات السرية لأصحاب العمل السابقين، أو الانتفاع بها علما بأن عقود العمل تنص أحيانا على ترتيبات خاصة بذلك الموضوع. على أنه إذا انطوى سلوك الموظف على خرق للعقد، أو إخلال بالتزام حفظ السرية أو سرقة أو اختلاس أو تجسس صناعي أو تواطؤ مع منافس معين، فإن كشف ذلك الموظف عن المعلومات أو انتفاعه بها يعتبر عملا غير مشروع قطعا[14].

ولا يعتبر من أعمال المنافسة غير المشروعة الكشف عن معلومات سرية أو الانتفاع بها على يد شخص كان قد حصل على تلك المعلومات إثر صفقة تجارية مشروعة مع مالكها الشرعي، شريطة ألا يترتب على ذلك الكشف أو الانتفاع أي إخلال بالعقد. على أن الكشف أو الانتفاع إذا تم بحسن نية فإن ذلك يدل عادة على أن المالك الشرعي لم يتخذ التدابير الكافية للحفاظ على سرية المعلومات، ولا يجوز له بالتالي الادعاء بحدوث منافسة غير مشروعة[15].

ومن المعلوم أن السر في تفوق شركة كوكاكولا الأمريكية في مواجهة الشركات التي تنافسها في مجال صناعة المياه الغازية يرجع إلى نجاحها في كتمان سر الوصفة الخاصة بالمادة التي تستعمل في صناعة مشروب الكوكاكولا، منذ مدة تزيد على قرن من الزمان وحتى الآن.

ومن الجدير بالذكر أنه في سنة 1977 أوقفت شركة كوكاكولا نشاطها في الهند لمشروب الكوكاكولا وسحبت استثماراتها لحماية الوصفة السرية[16]،. ويرجع السبب في ذلك إلى أن الحكومة الهندية طلبت من شركة كوكاكولا أن تبيع 60% من أسهم الشركة إلى مساهمين هنود، وأن تكشف للجانب الهندي عن الوصفة السرية لمشروب الكوكاكولا أو تنهى نشاطها في الهند تطبيقا للقانون الذي صدر آنذاك

الذي أوجب على الشركات الأجنبية التي تزاول نشاطها في الهند أن تتخلى عن الإدارة للجانب الهندي، كما ألزمها بنقل التكنولوجيا. وقد جادلت شركة كوكاكولا الحكومة الهندية وحاولت إقناعها – دون جدوى – بأن الوصفة السرية لمشروبها ليست تكنولوجيا، وإنما هي سر تجارى ومن ثم فهي لا تخضع لأي التزام وفقا للقانون الهندي المذكور بكشف الوصفة السرية. وأخيرا قررت الشركة إيقاف نشاطها في الهند وسحبت استثماراتها، إذ وجدت أن هذا القرار أفضل لها بكثير من كشف الوصفة السرية لمشروب الكوكاكولا ،على الرغم مما تكبدته من خسائر هائلة [17].

كما أن الشروط العقدية تعد من أهم وسائل تأمين المعلومات. فعادة تضع الشركات والمؤسسات ومراكز الأبحاث شروطا في العقود التي تبرمها مع العاملين والباحثين أو غيرهم من الأشخاص الذين تتيح لهم ظروف العمل معرفة الأسرار التجارية تتضمن إلزامهم بكتمان المعلومات وعدم الإفصاح عنها للغير أو استعمالها خارج نطاق العمل.

فلا ريب في أن الكشف عن المعلومات السرية أو الحصول عليها أو الانتفاع بها قد يهم أشخاصا غير من يجوز له الاطلاع عليها. وبصفة خاصة فقد يصل أحد المنافسين إلى حض أي موظف حالي أو سابق لدى المالك الشرعي للمعلومات على الكشف عنها بواسطة الإخلال مثلا بالتزاماته التعاقدية التي تربطه بالمالك الشرعي. ويقترن ذلك الحض غالبا باستمالة الموظف بطريقة غير مشروعة إلى ترك وظيفته وهو عمل يجوز اعتباره أيضا من أعمال المنافسة غير المشروعة [18].

كما تتضمن عقود نقل المعرفة الفنية – عادة – شروطا تلزم المرخص له بعدم إفشاء المعلومات السرية التي زوده بها المرخص.

فإذا لم يتخذ حائز المعلومات الإجراءات أو التدابير اللازمة ليحافظ على سرية المعلومات، سقط حقه في التمتع بالحماية التي يقررها القانون للأسرار التجارية [19].

وقد طبق القضاء الأمريكي هذا المبدأ في قضية Glaxo Inc. v. Novopharm Ltd. وتتلخص وقائع القضية التي رفعتها شركة Glaxo ضد شركة Novopharm كما جاء في عريضة الدعوى أن الشركة الأولى ادعت قيام الشركة الثانية (المدعى عليها) بتقليد أحد اختراعاتها الدوائية المحمية عن طريق البراءة، فضلا عن قيامها بسرقة أسرارها التجارية المتعلقة بخطوات وطريقة تحضير الدواء Zantac ومشتقاته، وهو ما يشكل منافسة غير مشروعة. وما يعنينا في القضية هو الشق الخاص بادعاء شركة Glaxo أن شركة Novopharm سرقت الأسرار المتعلقة بالعناصر والمكونات والخطوات الفنية التي تمر بها عملية تحضير الدواء واستخدمتها في إنتاج الدواء. وقد قضت المحكمة برفض هذا الادعاء استنادا إلى أن شركة Glaxo لم تقم باتخاذ التدابير اللازمة للمحافظة على سرية المعلومات المتعلقة بالعناصر الداخلة في تركيب الدواء وخطوات تحضيره، وذلك لأنها قامت بتقديم الوثائق والمستندات التي تتضمن تلك المعلومات إلى المحكمة في دعوى سابقة[20] بدون أن تتخذ أي إجراءات تكفل سريتها، فأتاحت لشركات إنتاج الأدوية الأخرى فرصة الاطلاع على هذه الوثائق والحصول على صور منها وبالتالي فقدت المعلومات طابع السرية. وكان يمكن للشركة أن تقدم الوثائق التي تحتوى على معلومات سرية في مظاريف مغلقة ومختومة وتطلب من المحكمة اتخاذ الإجراءات الكفيلة بالمحافظة على سريتها، ولكنها لم تفعل. وقررت المحكمة أن قيام الشركة المدعى عليها باستغلال هذه المعلومات التي أتيحت للكافة بعد قيام الشركة المدعية بإفشاء سريتها لا يعد سرقة للمعلومات، وأن عدم اتخاذ الشركة المدعية للإجراءات اللازمة للمحافظة على سرية المعلومات يسقط حقها في الحماية لأنها لم تعد أسراراً تجارية [21].

وقد يحدث أن يتم التوصل إلى السرية من قبل أشخاص آخرين، ولكن باستخدام طرق وتجارب وأبحاث علمية مشروعة، مع احتفاظ كل منها بسريتها واستخدامها على استقلال، فهل نحن هنا أمام انحسار السرية؟

الأقرب للقبول في هذا الفرض، أن صفة السرية تبقى قائمة بالرغم من تضاءل قيمتها الاقتصادية النسبية تبعا لمدى شيوعها بين المتنافسين، وتظل من ثم صالحة لحماية القانون، طالما ظلت غير مفصح عنها من قبل حائزيها واحتفظ كل منهم باستخدامها في طي الكتمان، ويرجع ذلك بالأساس إلى أنه لم يعد التوصل إلى هذه المعلومات يتم بطريقة فردية يصعب على الآخرين التوصل إليها، وإنما يمكن في ظل تدخل الأسلوب العلمي وتطبيق قواعد التخصص الدقيق في انجاز الأعمال والمحاولات المتتابعة والمستمرة في البحث العلمي، أن يتوصل في ذات الوقت إلى نفس المعلومة السرية أو إلى بعض مكوناتها، دون المساس بالصفة الجوهرية المتمثلة في السرية.

كذلك إذا تم الوصول إلى المعلومات السرية، استقلالا عن جهود صاحب المعلومات الأول، فإنه لا يمثل ثمة اعتداء على حقه في ضمان السرية على معلوماته، كما لا يتعارض ذلك مع ما توجبه الممارسات الشريفة في مجال التنافس الصناعي والتجاري. ولعل تفسير ذلك يرجع إلى أن الحماية القانونية للأسرار لا ترتب لحائزها حقا استئثاريا مطلقا حيث يجوز للغير استغلال هذه المعلومات السرية طالما أنه توصل إليها بطرق مشروعة عن طريق بذل الجهود الذاتية المستقلة، وذلك على خلاف الحقوق التي تترتب على براءة الاختراع .

ويلاحظ أن القضاء الفرنسي قد أخذ بهذا المفهوم، ففي حكم لمحكمة النقض الفرنسية قررت المحكمة أن توصل المنافسين إلى نفس المعلومات السرية في ذات الفترة الزمنية، لا يكون من شأنه أن يؤدي إلى انحسار السرية، ما ظلت الشركات المنافسة جاهلة لهذه المعلومات.

وبخصوص المحافظة على السرية في المجال التكنولوجي تواجهها صعوبات تتمثل في تحقيق التوازن بين المصالح المتعارضة لطرفي العقد، ولاسيما في مرحلة المفاوضات التي قد تنتهي إلى طريق مسدود دون التمكن إلى إبرام تعاقد بين الأطراف.

فمن جانب نجد أن طالب التكنولوجيا لديه الرغبة في معرفة الكثير من الخصائص المميزة للتكنولوجيا موضوع التعاقد، وذلك حتى يتمكن من معرفة القيمة الحقيقية للتكنولوجيا التي يرغب في شراءها، ومراعاة هذا المطلب العادل يقتضي السماح له بمعرفة أو الإطلاع على معلومات لها طابع السرية وذلك في المرحلة التي تسبق إبرام العقد.

وهناك مصلحة الطرف الآخر وهو مالك التكنولوجيا أو مالك السر، حيث أن لهذا الطرف مصلحة مشروعة في المحافظة على المعلومات السرية، والتي قد تجبر على الإفشاء بها إلى الطرف الآخر أثناء مرحلة المفاوضات وذلك بهدف التوصل إلى إبرام العقد وبدون السماح للطرف الآخر بالإطلاع على مقدار من السرية لا يمكن التوصل إلى معرفة حقيقة موضوع العقد ولن يتوصل الأطراف إلى أي اتفاق.

ومما يزيد الأمور تعقيدا هو أنه نظرا لعدم توافر الخبرة في طالب التكنولوجيا وخشية منه أن يقع ضحية لغبن فيما يتعلق بقيمة ما يعرض عليه من تكنولوجيا وأيضا رغبة منه في الحصول على تكنولوجيا متطورة وعدم قدرته على إجراء مقارنة أو تقييم لمزايا ما يعرض عليه، فإنه غالبا ما يلجأ لأهل الخبرة ويستعين بهم في مرحلة المفاوضات، كما هو الشأن في الحالات التي تتولى فيها البنوك تمويل المشروعات القائمة على التكنولوجيا محل العقد، وذلك حتى تطمئن هذه البنوك إلى استرداد أموالها في حالة نجاح المشروع.

ويلاحظ أن هذه العقبات التي تواجه الأطراف قد يترتب عليها الإخفاق في التوصل إلى إبرام العقد ومرجع ذلك أن الخبير الذي يستعين به طالب التكنولوجيا في مرحلة التفاوض إنما هو شخص أقدر من غيره على تقييم المعلومات السرية التي يطلع عليها، وبمعنى آخر انتقاص السر بمجرد الإطلاع عليه، وبالتالي يمكن أن يستفيد من هذه الفرصة بعد ذلك بمعرفته لهذه المعلومات السرية سواء كان ذلك لمصلحة طالب التكنولوجيا أو لمصلحته الشخصية، ومن هنا يمكن أن نتفهم

الاعتبارات المشروعة التي تجعل مالك السر يتردد ويتهيب كثيرا قبل الإفصاح عما لديه من معلومات ذات طابع سري .

إلا أنه من المألوف في العمل أن يحصل مالك السر من طالب التكنولوجيا على تعهد بعدم إفشاء الأسرار المحصل عليها أثناء المفاوضات، وعادة ما يقوم الطالب بالتوقيع على هذا التعهد ضمن الأوراق التي يرسلها مالك السر في المراحل التمهيدية للمفاوضات، إذ أن امتناع الطالب عن توقيع التعهد المذكور يمكن أن يؤدي إلى وقف المفاوضات قبل أن تبدأ، ويترتب على ذلك التعهد التزام الطالب وخبرائه سواء التابعين له مباشرة أو أولئك الخبراء الأجانب الذين تتم الاستعانة بهم لفحص التكنولوجيا بعدم الإفشاء. ويكون طالب التكنولوجيا مسؤولا عن التعويض في حالة عدم الالتزام بالمحافظة على السرية[22].

وفي إطار إجراءات المحافظة على السرية خلال مرحلة المفاوضات، فإن بعض الشركات الكبرى تصر على إجراء المفاوضات في مكاتبها وفي حضور عدد محدود جدا من خبراء كل من الطرفين حتى لا يحدث تسرب للمعلومات السرية، ومن ثم ترفض الشركات الكبرى إجراء المفاوضات في مكان آخر غير مكاتبها وتحت إشرافها وحراستها خوفا من تعرضها للسطو على أسرارها كأحد صور الجوسسة الصناعية.

كما تجري عادة هذه الشركات على عدم الإفصاح على جميع الأسرار، وبحيث لا يتم إفشاء إلا القدر الضروري جدا لتعريف طالب التكنولوجيا على جدوى التكنولوجيا له، وبحيث تكون المعلومات المصرح بها خلال المفاوضات غير كافية بذاتها لإدراك كافة الأسرار أو لاستغلالها.

وقد يطلب المالك من طالب التكنولوجيا تقديم كفالة مالية كخطاب ضمان مثلا أو القيام بإيداع مبلغ لدى أحد البنوك كضمانة، وذلك للتأكد من عدم الإخلال بشرط المحافظة على السرية، وبحيث يجوز للمالك القيام بتيسير خطاب الضمان مثلا إذا فشلت المفاوضات وأخل الطالب بالتزامه بالسرية وعدم الإفشاء.

أما إذا نجحت المفاوضات وتم إبرام العقد، فعادة ما تعتبر الكفالة المالية جزءا من الثمن الذي يدفع في مقابل التكنولوجيا[23].

وباعتبار أنه للمحافظة على الأسرار التجارية والمعلومات السرية يجب أن يحتاط بعدم إفشائها إلا لعدد قليل ممن يتعاملون معها. وهذا ما فعلته شركة كوكا كولا، فقد اتخذت إجراءات لحماية ثروتها الثمينة وهي الصبغة الخاصة بمنتوج الكوكا كولا، حيث أن الصيغة المكتوبة لهذا السر قد تم وضعها في خزينة بأحد البنوك في أطلنطا، وهذه الخزينة يتم فتحها فقط من قبل رؤساء ومديري الشركة وكذلك كانت سياسة الشركة أن اثنين فقط من الشركة هما اللذان يعلمان الصيغة في الوقت نفسه، ولهذين الشخصين الحق في الإطلاع على طريقة إعداد هذا المنتج وقد رفضت الشركة الكشف عن هوية هذين الشخصين، كما أنها لا تسمح لهذين الشخصين بالسفر معها في نفس الطائرة، وهذه الإجراءات يتم اتخاذها وإتباعها في جميع المنتجات الخاصة بإنتاج الشركة لمشروب الكوكا، وبذلك ظلت كل صيغة من الصيغ الخاصة بهذه المشروبات معروفة فقط لثلاثة أو أربعة أشخاص في الشركة، ونتيجة لذلك ظلت الصيغة الخاصة بالكوكا كولا سرا لفترة تزيد عن مائة عام.

<u>II – الحماية الوطنية:</u> أما عن القوانين الوطنية فنتناول في البداية القانون الأردني الذي لم يعرف هو بدوره الأسرار، ولكنه أورد في المادة 4 من القانون المتعلق بالمنافسة غير المشروعة والأسرار التجارية[24] بشروط هذه الأسرار والمتمثلة في:

"أنها غير معروفة في صورتها النهائية أو في مكوناتها الدقيقة، وليس من السهل الحصول عليها في وسط المتعاملين بها، كما أنها تكون ذات قيمة تجارية بسبب كونها سرية، وأنها خاضعة للإجراءات التي تكفل لها السرية، كما أنها لا تتعارض مع النظام العام أو آداب المجتمع الأردني".

أما بالرجوع إلى أمريكا صاحبة فكرة حماية الأسرار في المنظمة العالمية للتجارة والمبادرة بها كان المشرع الأمريكي هو أول من قنن تنظيم السرية فأصدر قانون السر التجاري الموحد والذي تمت الموافقة عليه في أوت عام 1979 وتم التوصية على تطبيقه في جميع الولايات وتم تعديله عام 1985.

والمجهود الأكبر لإصدار قانون حديث لحماية السرية كان عام 1993 في التنقيح الثالث لقانون المنافسة غير المشروعة والذي يشمل العديد من المواد المتعلقة بالأسرار التجارية وقد تم نشره عام 1995 بواسطة المعهد الأمريكي للقانون، وفي عام 1996 تم وضع قانون التجسس الاقتصادي EEA، وهو قانون جنائي[25]. ففيما يتعلق بالقانون الأمريكي فإن تعريف الأسرار التجارية فيه لبس واحدا، ذلك أن نظام حماية الأسرار التجارية في القانون الأمريكي مستمد من أكثر من مرجع، نذكر منها القانون الموحد لأسرار التجارة الأمريكي Uniform Trade secrets act (UTSA) ل 1979 فقد عرف الأسرار بأنها: "معلومات تشمل كل وصف ،تصميم أو مجموع أو برنامج أو أسلوب أو وسائل أو فن صناعي أو طريقة تكوين لها قيمة اقتصادية في حد ذاتها قائمة أو محتملة، نظرا لأنها غير معروفة عموما للأشخاص الذين يستطيعون الاستفادة من كشف هذه المعلومات أو استعمالها ولا يكون بإمكانهم الوصول إليها بسهولة بوسائل مشروعة تبذل جهود معقولة بسبب الظروف للحفاظ على سريتها".

وأمـــا قـــانـــون المنافســـة غيـــر المشروعـــة (التعديـــل الثـــالث 1995) The Restatement of unfair competition 1995(third) فقد توسعت في تعريفها للأسرار التجارية حيث جاء فيها: "سر التجارة هو أي معلومات يمكن استخدامها في مزاولة العمل أو في مشروع آخر، وتكون لها قيمة محل اعتبار وسرية، بحيث تعطي لصاحبها ميزة اقتصادية حالية أو محتملة في مواجهة غيره"[26].

ويتضح لنا مما تقدم أن الأسرار التجارية في القانون الأمريكي ليست هي تلك المعلومات الفنية فحسب، وإنما قد يمتد مفهومها إلى أي معلومة سواء فنية أو إدارية تمكن صاحب المعلومة من أن يتميز عن غيره في ميدان العمل.

ويلاحظ على التسميات والتعريفات أنها تدور في معظمها حول فكرة واحدة تستجمع شروط حماية السر التجاري، وصور تلك الأسرار على تنوعها.[27]

أما في فرنسا وعلى عكس ما هو عليه الحال في الولايات المتحدة، لا توجد تشريعات متعلقة بالسر التجاري، ويبقى القانون الوحيد في فرنسا الذي ينص صراحة على حماية السرية هو ذلك القانون الذي يحمي المعلومات والأسرار المتعلقة بالحياة الخاصة للأفراد دون أدنى حماية للأسرار التجارية والصناعية [28]. لذلك فإن الشركات والأفراد لديهم الحرية في اتفاقيات التوظيف في إيجاد تعريف خاص بهم للسر التجاري والفضل في ذلك يعود للمحكمة العليا الفرنسية التي وضعت تعريفا واسعا للسر التجاري، فقد عرفته بأنه: "أي وسيلة تصنيع أو صيغة أو آلة أو معلومات،... ذات قيمة اقتصادية أو عملية وتستخدم في الأعمال التجارية والتي تعطي صاحبها ميزة تنافسية على هؤلاء الذين لا يعرفونها"[29].

إلا أن هذه الوضعية التشريعية على وشك الانتهاء، بالنظر إلى مشروع القانون الذي صادق عليه المشرع الفرنسي في الآونة الأخيرة، والمتعلق بسر الأعمال[30].

وقد اقتدت فرنسا في ذلك بالعديد من الدول مثل: الولايات المتحدة الأمريكية ألمانيا، إيطاليا والتي تعتبر قوانينها بارزة في ميدان الأسرار.

وباعتبار أن التكييف الحالي للمساس بالأسرار في فرنسا هو: سرقة المعلومات خيانة الأمانة أو التقليد. فإن هذا التكييف يبقى عاجزا، كون المساس بالأسرار مسألة تقنية تستوجب نصوص خاصة و صريحة.

وحتى أمام التعديلات اللاحقة في فرنسا، يلاحظ بأن اقتراح القانون تشوبه بعض النقائص تستوجب الاستدراك مستقبلا، أهمها الاكتفاء بتجريم إفشاء السر دون النص على تجريم خرق السر وسرقته[31].

كما أنه في عام 1361 تم سن قانون في بريطانيا يمنع خرق السرية ويعاقب عليها بالحبس. وقد طورت عدد من الدول حماية متقدمة بعد هذا التاريخ، ففي عام 1776 سن البرلمان السويدي قانون الوصول إلى السجلات العامة، والذي ألزم كافة الجهات الحكومية التي لديها معلومات أن تستخدمها لأهداف مشروعة.

وفي العصر الحديث فإن مفهوم الحق في السرية ظهر في الإعلان العالمي لحقوق الإنسان عام 1948[32].

ثم تطور بعد ذلك الحق في السرية في الستينات نتيجة للتأثر بتقنية المعلومات

وبسبب القوى الرقابية المحتملة لأنظمة الكمبيوتر، التي استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة، وفي هذا الحقل فإن أول معالجة تشريعية في ميدان حماية البيانات كان عام 1970 في هيس بألمانيا[33].

وفي سنة 1981 وضع الاتحاد الأوربي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا إرشاديا لحماية السرية ونقل البيانات الخاصة، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الإلكترونية للبيانات، وهذه القواعد تصف البيانات والمعلومات السرية على أنها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع، التخزين، المعالجة والنشر.

ومفهوم حماية البيانات السرية في المواثيق المتقدمة والقوانين يتطلب أن تكون:

- قد تم الحصول عليها بطريق مشروع وقانوني.
- تستخدم للغرض الأصلي المعلن والمحدد.
- تتصل بالغرض المقصود من الجمع ولا تتجاوزه ومحصورة بذلك.
- صحيحة وتخضع لعمليات التحديث والتصحيح.
- تحفظ سرية و تحمى سرية.
- تدمر بعد استنفاذ الغرض من جمعها[34].

وبالرجوع للتشريع الجزائري نجده ينص في المادة 07 من القانون 90-11 المتعلق بعلاقات العمل[35] أنه من بين الواجبات الأساسية التي يخضع لها العمال في إطار علاقات العمل أن لا يفشوا المعلومات المهنية المتعلقة بالتقنيات والتكنولوجيا وأساليب الصنع وطرق التنظيم وبصفة عامة أن لا يكشفوا مضمون الوثائق الداخلية الخاصة بالهيئة المستخدمة إلا إذا فرضها القانون أو طلبتها سلطتهم السلمية.

وما يلاحظ على المشرع هنا، أنه بداية خصص المجالات التي تتعلق بها المعلومات المهنية وهي: التقنيات، التكنولوجيا، أساليب الصنع وطرق التنظيم ويلاحظ بأنها جاءت شاملة للأسرار التجارية والصناعية والمعرفة الفنية، ثم أطلق الأمر على عمومه وجعل المعلومات المهنية السرية متضمنة في الوثائق الداخلية الخاصة بالهيئة المستخدمة.

وقد أطلق المشرع قبل ذلك على هذا النوع من الوثائق المتضمنة للسرية عبارة "الوثائق المصنفة" من خلال المرسوم رقم 84-287 المحدد للتدابير المخصصة لحماية الوثائق المصنفة[36].

حيث اعتبر الوثيقة المصنفة أي مكتوب أو رسم أو مخطط أو خريطة، أو صورة، أو شريط صوتي، أو فيلمي، أو أي وثيقة أو سند مادي يتضمن معلومات تجب حمايتها[37].

وقد ربط المشرع السرية بدرجة حساسيتها وقسمها إلى أربعة أصناف وهي "سري جدا"، "سري"، "كتماني"، "توزيع محدود"

حيث تصنف فئة "سري جدا" الوثائق التي يلحق إفشاؤها خطرا بالأمن الوطني وتصنف في فئة "سري" الوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الأمة ويساعد بلدا أجنبيا.

أما فئة كتماني "تصنف في ظلها الوثائق التي يلحق إفشاؤها ضررا بأحد الأعمال الحكومية أو إحدى الإدارات أو الهيئات أو الشخصيات السياسية

الجزائرية. وأخيرا فئة "توزيع محدود" تصنف فيها الوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الدولة، ومن ثم لا يجوز أن يطلع عليها إلا الأشخاص المؤهلون[38].

كما نجد المادة 27 من القانون 04-02 المتعلق القواعد المطبقة على الممارسات التجارية حظر الاستفادة من الأسرار المهنية بطريقة غير مشروعة.

وقد جاء ذلك كما يلي:

"...4- إغراء مستخدمين متعاقدين مع عون اقتصادي منافس خلافا للتشريع المتعلق بالعمل.

5- الاستفادة من الأسرار المهنية بصفة أجير قديم أو شريك للتصرف فيها قصد الإضرار بصاحب العمل أو الشريك القديم".

__الخاتمة :__ لقد رأينا بأن الإطار القانوني لأمن المعلومات، ينطوي على نوعين من الحماية، الحماية الوطنية و الحماية الدولية.

وما يلاحظ عن هذه الحماية، أن المعلومات السرية تحمى بواسطة نظام الاسرار التجارية والصناعية كطريق بديل لبراءات الاختراع، لأن الحماية بمقتضى براءة الاختراع تلزم صاحب المعلومة بإفشاء السرية، مقابل الحماية لمدة 20 سنة –وبعد هذه المدة تسقط البراءة في الميدان العمومي –، وذلك على عكس حماية المعلومات بمقتضى نظام الاسرار التجارية والصناعية، والتي يبقى صاحبها متمتع بالحماية ما دامت السرية قائمة، وإلى غاية إفشاءها.

الأمر الذي أدى إلى تضارب المواقف بين المؤيد والمعارض، بحسب مصلحة كل منهما.

__الهوامش:__

1- حيث وجدت الدول الكبرى أن تدعيم حقوق الملكية الفكرية وترسيخها على المستوى الدولي بالقدر الذي يتفق مع مصالحها يصعب أن يتحقق عن طريق الاتفاقيات الدولية التي تبرم تحت رعاية المنظمة العالمية للملكية الفكرية (الويبو).

2- حيث أنه لم يكن من الجائز – وفقا للاقتراح الأمريكي – استعمال البيانات أو المعلومات التي تقدم إلى الجهات الحكومية بما يحقق مصلحة الغير إلا في الظروف القهرية المتعلقة بالصحة العامة، وبعد تعويض صاحب المعلومات بالكامل بما يماثل القيمة السوقية للمعلومات التي يستفيد بها الغير.

3- الوثيقة:MTN.GNG/NG11/W/ 68

4- الوثيقة:MTN.GNG/NG11/W/ 70

5- الوثيقة: MTN.GNG/NG11/W/71

6- الوثيقة: MTN.GNG/NG11/W/73

7- الوثيقة: MTN.GNG/NG11/W/74

8- الوثيقة: MTN.GNG/NG11/W/75

9- في بعض البلدان كالولايات المتحدة الأمريكية واليابان، فالمجهودات المبذولة من طرف مالك المعلومة السرية تعتبر لدى المحاكم شرطا أساسيا للتوصل إلى كون المعلومة تطبعها السرية من عدمها، أي أن العبرة بالتدابير المتخذة للحفاظ على السر، وذلك ما سوف نتطرق له في الشرط الأخير.

10 -Protection contre la concurrence déloyale, op. cit, 1994 .

11- انظر: حسام الدين عبد الغني الصغير، ندوة الويبو الوطنية عن الملكية الفكرية، حماية المعلومات غير المكشوف عنها بناء على اتفاق تريبس، القاهرة، من 17 إلى 19 فيفري 2003 .

12- ونجد هذا واضحا في الولايات المتحدة الأمريكية في مدونة المسئولية عن الفعل الضار لسنة 1939 حيث عرفت سر التجارة في القسم 757 من قانون التجارة بأنه أي وصف أو تصميم أو أسلوب أو مجموعة من المعلومات التي تستعمل في العمل، فتعطي لصاحبها فرصة الحصول على ميزة نسبية في مواجهة منافسيه الذين لم يسبق لهم استعمالها.

13 –Article 6 alinéa 1 des dispositions types sur la protection contre la concurrence déloyale, op. cit, 1996 .

14-Article 6 alinéa 2 des dispositions types sur la protection contre la concurrence déloyale, op. cit, 1996 .

15 - Paris (14éme ch ., sect.B), 16 juin 2000, Petites affiches, 2001, n°58, p 14 note : Marie MALAURIE- VIGNAL .

16- و ذلك على الرغم من مزاولة الشركة لنشاطها في الهند منذ مدة تزيد عن خمسة وعشرين عاما سابقة، وكبر حجم السوق الهندي التي تضم حوالي 550 مليون شخص يشربون الكوكاكولا .

17 - أكثر تفاصيل بخصوص القضية نجدها بموقع الأنترنت : www.carolinapatents.com .

18-Article 6 alinéa 1 des dispositions types sur la protection contre la concurrence déloyale, op. cit, 1996.

19 -C Paris, 5 éme ch, 12 juin 1998, expertises, n° 225, avril 1999, p 107, note : Nathalie BOULVARD.

20- وهى تتكون من 135 مستندا.

21-Glaxo Inc. V.Novapharm Ltd., 1996 U.S .Dist. (Easternt District of North Carolina, July 5, 1996) .

تفاصيل القضية نجدها بموقع الأنترنت : www.carolinapatents.com .

22-جلال وفاء محمدين، الإطار القانوني لنقل التكنولوجيا، دار الجامعة الجديدة، 2004، ص19.

23- وإذا كان المالك يحتاط لنفسه بتطلب الكفالة المالية ضمانا لعدم إفشاء السرية أثناء المفوضات، فإن على الطالب كذلك يتحوط لنفسه فيتنحى الحذر بأخذ التدابير الكفيلة لاسترداد قيمة الكفالة المقدمة منه إذا ما فشلت المفاوضات -دون إخلال بالسرية - بأن ينص في التعهد المقدم منه بالالتزام بعدم الإفشاء على كيفية وميعاد استرداد الكفالة.

24 - المـــادة 4 من قـــانون المنافســـة غير المشروعـــة والأسرار التجارية الأردني رقم 15 لسنة 2000.

25- وهنا فقد تحركت الحكومة الفيدرالية لحماية حقوق الملكية الخاصة في أسرار التجارة، وكان من أهم الأسباب لتشريع هذا القانون هو محاولة الحكومات الأجنبية الوصول إلى الأسرار التجارية للشركات الأمريكية.

أمال زيدان عبد الله، الحماية القانونية للأسرار التجارية في عقود نقل التكنولوجيا، دار النهضة العربية 2009، ص 14.

26- التعاريف المقدمة كانت في ظل قوانين خاصة، أما إذا انتقلنا إلى الشريعة العامة والمتمثلة في قانون الفعل الضار لعام 1939 وفي المادة 757 منه نجدها تنص على أن "السر التجاري هو أي وصف أو تصميم أو أسلوب أو مجموعة من المعلومات التي تستعمل في العمل فتعطي لصاحبها ميزة في مواجهة منافسيه الذين يجهلونها، أو لم يسبق لهم استعمالها".

27– عمر كامـــل السواعـــدة، الأســـاس القانونـــي لحماية الأســـرار التجارية، دار الحامد 2009، ص 39.

28 - François MOULIERE, Secret des affaires et vie privée, Recueil Dalloz – 1er mars 2012, n°09, p.571.

29– أمال زيدان عبد الله، الحماية القانونية للأسرار التجارية في عقود نقل التكنولوجيا، دار النهضة العربية 2009، ص59.

30– حيث صادق المشرع الفرنسي في 23 جانفي 2012 من خلال القراءة الأولى على اقتراح قانون متعلق بسر الأعمال واستحدث جنحة جديدة تتمثل في جنحة افشاء سر الأعمال.

وكان ذلك من خلال المواد 325 وما يليها، التابعة للفصل 07 من الباب 02، المندرج تحت الكتاب 03 للقانون الجنائي الجديد، الذي اعتبر بأن افشاء الأسرار يعتبر جنحة يعاقب عليها بثلاث سنوات حبس وغرامة قدرها 375000 euro.

وقد اعتبر Bernard CARAYON محرر هذه النصوص المتعلقة بأسرار الأعمال، على أن هذه الوضعية التشريعية تعتبر حتمية أمام فرنسا، حتى تستجيب للمقتضيات الوطنية والدولية، وأهمها ما تمليه اتفاقية تربس.

A.ASTRAIX, violation du secret des affaires : création d'un délit, Recueil Dalloz - 02 fevrier 2012, n°5, p.286.

31- Anne COUSIN, vers une protection accrue du secret des affaires, Recueil Dalloz-12 juillet 2012, n° 27, p.1808.

32– حيث تنص المادة 12 منه على أنه: "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في الحماية من مثل هذا التدخل أو تلك الحملات".

33– ثم تبعه سن قانون وطني في السويد عام 1973، ثم الولايات المتحدة الأمريكية سنة 1974 ثم فرنسا عام 1978.

34– انظر: يونس عرب، منتدى العمل الإلكتروني، الخصوصية وأمن المعلومات، اتحاد المصارف العرب، عمان، من 20 إلى 22 جانفي 2001 .

35– الرجوع للمادة 7 من القانون رقم 90–11 المؤرخ في 21 أفريل 1990 والمتعلق بعلاقات العمل، وقد وردت هذه المادة تحت عنوان الفصل الثاني: واجبات العمال، الوارد بدوره تحت الباب الثاني: حقوق العمال وواجباتهم.

36- مرسوم رقم 84-287 المؤرخ في 22 ديسمبر 1984، المحدد للتدابير المخصصة لحماية الوثائق المصنفة، ج ر، رقم 69.

37- المادة 02 من المرسوم رقم 84-387.

38- المادة 03 من المرسوم رقم 84-387.

إشكالية القانون الواجب التطبيق على النزاعات الإلكترونية

د. تدريست كريمة

جامعة مولود معمري، تيزي-وزو

مقدمة: لاشك أن العصر الذي نعيش فيه هو عصر المعلوماتية وثورتها، وأن أبرز مقومات هذه الثورة شبكة الإنترنت التي تفوق في آثارها المذهلة، ما صاحب الثورة الصناعية من تقدم وازدهار في شتى المجالات.

وقد ترتب عن ظهور هذه الثورة المعلوماتية أن بدا في الأفق نوع جديد من المعاملات القانونية يتم عبر شبكة الإنترنت، يسمى بالمعاملات الإلكترونية وهي معاملات تتم عن بعد، بين أشخاص ينتمون إلى دول مختلفة عبر شبكة لا تتقيد بالحدود الجغرافية التي تفصل الدول، كما تتم في مجال افتراضي ليس له أدنى مرتكزات جغرافية، وتتسم هذه المعاملات بالطابع الدولي لأنها من جهة – وكما تقدم– تتم بين أطراف يتواجدون في دول مختلفة، ومن جهة أخرى، هناك من يذهب إلى إضفاء صفة الدولية على جميع المعاملات التي تتم عبر شبكة الإنترنت حتى وإن تمت بين أطراف من دولة واحدة، لأن هذه الشبكة هي دولية بطبيعتها.

ونظرا لكثرة مثل هذه المعاملات الإلكترونية التي تتم عبر شبكة الإنترنت، فمن البديهي أن تكثر النزاعات الناشئة عنها، والتي تتسم بالطابع الدولي – لأنها ناشئة عن معاملات الكترونية دولية–، الأمر الذي يثير العديد من المشكلات في القانون الدولي الخاص، لا سيما مشكلة تحديد القانون الواجب التطبيق عليها.

لا يخفى أن القانون الدولي الخاص يرتكز في حل مشكلة القانون الواجب التطبيق على العلاقات القانونية التي يتخللها عنصر أجنبي، على منهجية تنازع القوانين التي تعد حجر الزاوية له، وعليه، نتساءل عن مدى إمكانية إعمال منهج

قاعدة التنازع لحل مشكل القانون الواجب التطبيق على النزاعات الإلكترونية؟ (المبحث الأول).

غير أن البعض يذهب إلى اعتبار قواعد القانون الدولي الخاص التقليدية القائمة على منهج قاعدة التنازع، متخلفة عن مجاراة الوثبات السريعة التي أحدثها التعامل عبر شبكة الإنترنت، ومن ثم تحتاج إلى تعديل وتطوير حتى تظل صالحة لمواجهة هذا العالم الجديد، عالم تكنولوجيا المعلومات والاتصالات، الأمر الذي أدى إلى المناداة بضرورة إيجاد منهج آخر يتلاءم مع هذه المستجدات، فكان الحل المقترح هو تطبيق منهج القواعد المادية الإلكترونية. (المبحث الثاني).

المبحث الأول

نزاعات المعاملات الإلكترونية ومنهج قاعدة التنازع الدولي للقوانين

حين نشوب أي نزاع بشأن المعاملات الإلكترونية، فمن الضروري معرفة القانون الواجب التطبيق عليها، وبإعمال منهج قاعدة التنازع الدولي للقوانين لتحديد هذا القانون، سيتم إخضاع مثل هذه المعاملات لقواعد الإسناد التقليدية، لاسيما في ظل غياب قواعد إسناد خاصة بتلك النوعية من المعاملات. (المطلب الأول)

لكن أمام خصوصية هذه المعاملات، لقي تطبيق منهج قاعدة التنازع عليها جملة من الانتقادات، من الأهمية استعراضها مبرزين التحديات التي تثيرها هذه المعاملات في مجال تحديد القانون الواجب التطبيق عليها. (المطلب الثاني)

المطلب الأول

تطبيق منهج قاعدة التنازع على المعاملات الإلكترونية

كثيرة ومتنوعة هي المعاملات الإلكترونية التي تتم عبر شبكة الإنترنت، والتي تنقسم كما هو الشأن في المعاملات التقليدية إلى معاملات تعاقدية وأخرى غير تعاقدية، مما يستتبع نشوب العديد من النزاعات. سيتم بداية تطبيق منهج قاعدة التنازع على التعاقدية منها (الفرع الأول) ومن ثم غير التعاقدية (الفرع الثاني). مع

التركيز على أهم المعاملات التي تجرى على الشبكة وبخاصة تلك التي تثير تحديات في تطبيق هذا المنهج.

الفرع الأول

منهج قاعدة التنازع والالتزامات الإلكترونية التعاقدية

لمن المستقر عليه لدى غالبية النظم القانونية المقارنة، خضوع العقود الدولية الخاصة لقانون الإرادة كقاعدة عامة[1]، (أولا) مع إيراد استثناءات عليها (ثانيا) وهو ما ينعكس على العقود الإلكترونية الدولية لا سيما تلك التي تجرى على شبكة الإنترنت.

أولا- القاعدة العامة في تطبيق قانون الإرادة:

يقصد بمبدأ اختصاص قانون الإرادة بحكم العقود الدولية الخاصة؛ احترام إرادة المتعاقدين أخذا بمبدأ سلطان الإرادة[2]، أي إخضاع عقودهم للقانون الذي يختارونه. ولقد تبنت معظم القوانين الوطنية المقارنة هذا المبدأ وعلى غرارها القانون الجزائري وهو ما يتجلى من قاعدة التنازع الواردة في نص المادة 18 من القانون المدني الجزائري المعدل والمتمم[3]، التي تنص في فقرتها الأولى على أنه: «***يسري على الالتزامات التعاقدية القانون المختار من المتعاقدين*** ***إذا كانت له صلة حقيقية بالمتعاقدين أو بالعقد.***».

على الرغم من استقرار قاعدة حرية اختيار الأطراف للقانون الواجب التطبيق على عقدهم الدولي، كما تقدم ذكره، إلا أن تطبيق هذه القاعدة قد أثار جدلا فقهيا واسعا حول حدود ممارسة الأطراف لحريتهم العقدية؛ فهل اختيار أي قانون يعتد به؟

انقسم الفقهاء في الاجابة عن هذا السؤال إلى ثلاث اتجاهات[4]؛ ذهب الاتجاه الأول إلى التضييق من نطاق هذا القانون وقصره على القوانين الوطنية الصادرة عن دولة معينة تتمتع بهذا الوصف طبقا لأحكام القانون الدولي العام. في حين يوسع اتجاه ثان من نطاقه، بحيث لا يشترط أن يكون القانون المختار قانون دولة

معينة، بل يجوز اسناد العلاقة العقدية لقواعد لا تنتمي إلى نظام وطني معين، كتلك القواعد العرفية التي استقرت في مجال التجارة الدولية. بينما اتخذ اتجاه آخر موقفا وسطا؛ فهو اتجاه معتدل يخول المتعاقدين حرية اختيار القانون الواجب التطبيق على عقدهم الدولي، لكن يحرص في ذات الوقت على ألا تصل هذه الحرية إلى حد إطلاق حرية المتعاقدين في اختيار قانون على نحو قد يؤدي إلى الغش نحو القانون أو الإفلات من الأحكام الآمرة في القوانين المختارة.

وبالعودة إلى قواعد التنازع الجزائرية لاسيما نص المادة المذكور أعلاه، يلاحظ أن القانون الجزائري يقيد حرية المتعاقدين في اختيار قانون العقد باقتضاء "**توافر صلة جادة وحقيقية بين القانون المختار والعقد أو بالمتعاقدين**"، وهو موقف غالبية القوانين الوطنية المقارنة التي تحرص في عمومها على عدم مخالفة النظام العام والآداب العامة في اختيار المتعاقدين، وألا يكون خيار المتعاقدين منطويا على غش أو تحايل على القانون[5].

وبالتالي فإن تطبيق قانون الإرادة على العقد الدولي الإلكتروني وفقا للاتجاه الأول سيؤدي الى تطبيق قوانين وطنية داخلية، في حين يؤدي تطبيق الاتجاه الثاني إلى تطبيق القواعد والأعراف التي استقرت في مجال التجارة الإلكترونية[6]، بينما يثير تطبيق الاتجاه الثالث اشكال لصعوبة البحث عن الصلة بين القانون المختار والعقد في مجال الإنترنت، لأن اثبات هذه الصلة في ظل العقود الدولية الخاصة التقليدية انما يعتمد على عناصر مادية، كمكان إبرام العقد أو تنفيذه، لا تصلح لبيئة الإنترنت. لذلك ذهب فقهاء قانون التجارة الإلكترونية إلى انه لا يشترط ان تكون هذه الصلة قائمة على عناصر مادية أو شخصية، بل يكفي أن توجد صلة فنية، كأن يتم العقد في صورة عقد نموذجي متعارف عليه في مجال التجارة الإلكترونية[7].

بالإضافة إلى ما ذكر عن اختيار قانون الإرادة، يثار التساؤل عن كيفية التعرف على إرادة المتعاقدين لتحديد قانون الإرادة؛ وهل يمكن الاعتداد بالإرادة الضمنية

أو المفترضة للمتعاقدين في حالة عدم وجود إرادة صريحة لهما بشأن اختيار القانون الذي يحكم عقدهما؟

إن البحث عن نية أطراف العلاقة التعاقدية فيما يتعلق بالقانون الواجب التطبيق لا يثير الاشكال حينما يكون الأطراف قد نصوا صراحة في عقدهم على اختيار قانون معين لحكمه[8]. لذلك، علّق جانب من الفقه تطبيق قانون الإرادة في مجال العقود الدولية، على شرط أن يعبر الأطراف عن اختيارهم لهذا القانون صراحة[9]؛ ويتم ذلك من خلال إدراج شرط في العقد يحدد فيه الأطراف القانون الواجب التطبيق على عقدهم، ويسمى "شرط الاختصاص التشريعي"[10]. وهو الشرط الذي صار مألوفا في عقود التجارة الإلكترونية المبرمة عبر الإنترنت، لأنها تبرم وفق عقود نموذجية متعارف عليها في هذا المجال، تنطوي على بند يحدد فيه الأطراف القانون الواجب التطبيق على عقدهم، ويخضع العقد للقانون المختار دون اشتراط وجود أية صلة حقيقية أو جادة بين القانون المختار والعقد[11].

لكن قد يتجاهل الأطراف تحديد القانون الواجب التطبيق على عقدهم بصورة صريحة، أو أن تكون إرادتهم غير واضحة، فيرى جانب من الفقه[12] أنه ينبغي البحث عن إرادتهم الضمنية، وذلك باستخلاص نيتهم وتوجههم وميلهم نحو قانون معين، من ظروف الحال وملابسات العملية التعاقدية[13]، لأن الاختيار الضمني هو اختيار حقيقي ولكنه غير معلن[14].

ولقد أخذت العديد من القوانين المقارنة بالإرادة الضمنية في اختيار قانون العقد الدولي، كالقانون المصري مثلا[15]، وهذا خلاف ما هو عليه الحال في القانون الجزائري، إذ أن نص المادة 18 السالفة الذكر، لم يتضمن أية عبارة تفيد الأخذ بالإرادة الضمنية، مما يعني أن قواعد التنازع الجزائرية لا تعتد إلا بالإرادة الصريحة في اختيار القانون الذي يحكم العقود الدولية الخاصة[16].

ومن كل ما تقدم فإن تطبيق قانون الإرادة على العقود الإلكترونية الدولية، يكون في حالة اتفاق الأطراف صراحة أو ضمنا حول اختيار القانون الواجب التطبيق

على عقدهم، أما إذا لم يوجد مثل هذا الاتفاق، فيجب على القاضي الاستعانة بضوابط الاسناد الاحتياطية التي تنص عليها قواعد التنازع في قانونه الوطني وذلك لتحديد القانون الواجب التطبيق على النزاع المعروض عليه بشأن العقد الإلكتروني الدولي وهذا إذا تخلف الضابط الأساسي المتمثل في قانون الإرادة.

ثانيا- الاستثناءات: تطبيق ضوابط احتياطية

إذا انعدمت الإرادة الصريحة للمتعاقدين حول اختيار القانون واجب التطبيق على العقد المبرم عبر الإنترنت وتعذر الكشف عن نيتهم الضمنية فيتعين على القاضي البحث عن القانون الواجب التطبيق، وهنا نتساءل هل للقاضي الحرية في اختيار هذا القانون وبالتالي إمكانية تطبيق قانونه الوطني.

يرى غالبية فقهاء القانون الدولي الخاص أنه يتعين على القاضي بصدد تحديده للقانون الواجب التطبيق الاستناد على ضوابط موضوعية ذات صلة وثيقة بالعقد أهمها قانون دولة ابرام العقد أو قانون دولة تنفيذه أو قانون موطنهما المشترك(17).

وبالرجوع إلى قواعد التنازع الجزائرية، يلاحظ أن المشرع الجزائري إلى جانب وضعه ضابط أساسي في اختيار القانون الواجب التطبيق على العقد الدولي والمتمثل في الأخذ بقانون الإرادة، فقد أقرّ ضوابط احتياطية يلجأ إليها القاضي إذا انعدمت الإرادة، وهو ما يستفاد من نص الفقرتين الثانية والثالثة من المادة 18 السالفة الذكر، اللتان تنصان على أنه:

« **في حالة عدم إمكان ذلك، يطبق قانون الموطن المشترك أو الجنسية المشتركة.**

وفي حالة عدم إمكان ذلك، يطبق قانون محل إبرام العقد».

يتضح من هاتين الفقرتين أنه إذا لم يختار المتعاقدين القانون الواجب التطبيق أو كان هذا الأخير غير ذي صلة حقيقية بالعقد أو بالمتعاقدين، فإن القاضي يطبق قانون الموطن المشترك للمتعاقدين أو الجنسية المشتركة، وفي حالة عدم إمكان ذلك، يطبق قانون محل إبرام العقد.

على الرغم من أهمية هذه الضوابط لاسيما ضابط محل إبرام العقد الذي يعد من أهم الضوابط الاحتياطية المعمول بها في مجال تحديد القانون الواجب التطبيق على العقود الدولية الخاصة التقليدية، غير أنه يصعب تطبيق هذا الضابط في مجال العقود الإلكترونية التي تبرم عبر شبكة الإنترنت.

الفرع الثاني

منهج قاعدة التنازع والالتزامات الإلكترونية غير التعاقدية

يقصد بالالتزامات غير التعاقدية الالتزامات الناشئة عن الفعل الضار الذي تبنى عليه المسؤولية التقصيرية، والالتزامات الناشئة عن الفعل النافع؛ كالإثراء بلا سبب، الفعل النافع[18]. غير أن الملاحظ أن أكثر ما يثار بخصوص النزاعات المترتبة عن الالتزامات الإلكترونية غير التعاقدية، تتعلق بتلك الناشئة عن الفعل الضار لذا سنقتصر البحث مسألة القانون الواجب التطبيق عليها، وذلك بإخضاعها لمنهج قاعدة التنازع الدولي للقوانين.

تجمع غالبية النظم القانونية المقارنة، على اختصاص القانون المحلي بحكم المسؤولية عن الفعل الضار، وذلك كقاعدة عامة، (أولا)، غير أن تطبيق هذه القاعدة يثير العديد من الصعوبات واجهت ولا تزال تحديد القانون الواجب التطبيق على نزاعات المسؤولية التقصيرية عندما تتوزع عناصر هذه المسؤولية في أكثر من مكان، ولا شك أن هذه الصعوبات تكون أكثر تعقيدا فيما يتعلق بتحديد القانون الواجب التطبيق على المسؤولية عن الفعل الضار المرتكب عبر شبكة الإنترنت لذا يظهر من الضروري التعرف على القانون الواجب التطبيق على بعض الأنماط الضارة التي ترتكب على الشبكة والمنطوية على خصوصية (ثانيا).

أولا- القاعدة العامة في اختصاص القانون المحلي: يرتب القانون على الأفعال الضارة مسؤولية مدنية تعطي المتضرر حق المطالبة بالتعويض، وبخصوص القانون الواجب التطبيق في هذا الصدد، فيلاحظ أن التنازع بشأنه يدور بين قانون محل ارتكاب الفعل الضار وقانون المحكمة المرفوع أمامها النزاع. ولقد اتجهت

قواعد الاسناد لدى غالبية التشريعات الوطنية المقارنة إلى اسناد الاختصاص لقانون البلد الذي وقع فيه الفعل الضار[19]، وهو ما كرسه القانون المدني الجزائري في المادة 20 منه التي تنص على ما يلي: « **يسري على الالتزامات غير التعاقدية قانون البلد الذي وقع فيه الفعل المنشيء للالتزام.».**

ويبرر اختصاص القانون المحلي على اعتبار أن الأفعال الضارة تشكل خرقا لقواعد سلوك الأفراد في المجتمع الذي حدثت فيه، كما أن هذه القواعد تعد من قواعد الأمن المدني ومتعلقة بالنظام العام[20]، ومن ثم فإن تقدير مدى مخالفة قواعد السلوك في مجتمع ما يقدر في ضوء أحكام قانون ذلك المجتمع الذي ارتكب فيه الفعل الضار؛ فبمقتضى هذا القانون يقدر حجم الضرر ومقدار التعويض الواجب دفعه لجبر الضرر واصلاحه[21].

لا يثير إعمال ضابط القانون المحلي صعوبة في التطبيق متى وقع الفعل الضار في نفس البلد الذي يتحقق فيه الضرر، ولكن الإشكالية التي تثار تتمثل في صعوبة تحديد البلد أو الإقليم الذي وقع فيه الفعل المنشيء للالتزام إذا ما وقع الفعل في بلد وتحقق الضرر في بلد آخر[22]. لذلك يثور التساؤل عن القانون الواجب التطبيق في هذه الحالة؟

اختلف الفقه في الإجابة عن هذا التساؤل؛ فذهب اتجاه منه إلى تطبيق قانون مكان ارتكاب الفعل الضار بغض النظر عن مكان تحقق الضرر. ويبرر هذا الاتجاه موقفه على أساس أن الخطأ هو عماد المسؤولية التقصيرية، إذ أن القواعد المنظمة للمسؤولية تعد من قواعد تأمين المجتمع التي تهدف إلى منع وقوع الخطأ التقصيري، كما أن تطبيق هذا القانون يتلاءم مع توقعات مرتكب الفعل، حيث يكون على علم بأحكام هذا القانون[23].

بينما ذهب اتجاه آخر إلى تطبيق قانون مكان تحقق الضرر، وذلك لأن قواعد المسؤولية التقصيرية غايتها الأولى التعويض المدني لا العقوبة على الفعل الضار كما أن مكان الضرر هو عادة مكان موطن أو محل إقامة المضرور، وهذا الأخير

هو الطرف الضعيف الذي يجب حمايته وذلك بتطبيق قانون المكان الذي تحقق فيه الضرر[24].

لقد انتقد كلا الرأيين السابقين على أساس أن الاقتصار على الأخذ بقانون مكان ارتكاب الفعل الضار وحده، أو قانون مكان تحقق الضرر وحده، لا يحقق اعتبارات العدالة؛ لذلك ينبغي الأخذ بمعايير أكثر مرونة في تحديد القانون الواجب التطبيق، بتطبيق قانون الدولة التي وقع فيها أكثر عناصر الاعتداء اعتبارا[25].

ولا يتوقف الإشكال في تحديد القانون الواجب التطبيق في مجال الأفعال الضارة المرتبة للمسؤولية التقصيرية على ما ذكر، وانما يتوقف بداءة على تكييف الفعل ذاته إن كان ضارا أو غير مشروع بموجب أحكام قانون القاضي المعروض عليه دعوى المسؤولية؛ إذ تقيد العديد من التشريعات قاعدة اختصاص القانون المحلي بشرط عدم مشروعية الفعل في القانون الوطني للقاضي. وهذا ما تقضي به قواعد التنازع الجزائرية، فبعد أن كرس المشرع الجزائري في المادة 20 الفقرة الأولى من القانون المدني، المذكورة أعلاه، قاعدة اختصاص قانون البلد الذي وقع فيه الفعل المنشيء للالتزام، عاد في الفقرة الثانية من المادة ذاتها ليقيد اعمال القانون الأجنبي: « **غير أنه فيما يتعلق بالالتزامات الناشئة عن الفعل الضار، لا تسري أحكام الفقرة السابقة على الوقائع التي تحدث في الخارج وتكون مشروعة في الجزائر وإن كانت تعد غير مشروعة في البلد الذي وقعت فيه.**». فكون الفعل يعد غير مشروع وفقا لقانون البلد الذي وقع فيه، فإن ذلك لا يعد كافيا حتى لاستكمال عناصر المسؤولية التقصيرية، بل يشترط بالإضافة إلى ذلك أن يعتبر غير مشروع وفقا للقانون الجزائري.

وإذا كان الأمر كما تقدم، فإن الأمر يزيد تعقيدا بالنسبة للأفعال الضارة التي ترتكب على شبكة الإنترنت، فالمشكلة تتعدى مسألة افتراق مكان ارتكاب الفعل الضار عن مكان تحقق الضرر، فالأفعال الضارة على الشبكة تعرف تعددا لأماكن تحميل المواد المخالفة، وتعدد أماكن الضرر المباشر، وصعوبة تحديد المخطئ من

بين المشتركين في تقديم خدمات المعلومات[26]...الخ، كل ذلك يستدعي التعرف على بعض صور الأعمال الضارة التي ترتكب عبر الإنترنت، والإشكالات التي تثيرها بالنسبة للقانون الواجب التطبيق.

ثانيا- بعض صور الأعمال الضارة التي ترتكب عبر الإنترنت:

تتمثل غالبية الأعمال الضارة التي تطرح على شبكة الإنترنت في: الإساءة إلى السمعة والاعتداء على حقوق الشخصية،(1) والاعتداء على حقوق الملكية الفكرية(2).

1- الإساءة إلى السمعة والاعتداء على حقوق الشخصية: إن الأفعال الضارة التي يمكن أن ترتكب عبر الشبكة الدولية للاتصالات متعددة، كالاعتداء على الحياة الخاصة، نشر رسائل تتضمن الإساءة إلى السمعة،[27] كما يستطيع قراصنة الحاسب الآلي التوصل إلى المعلومات المالية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة[28]. وهنا يذهب بعض الفقه[29] إلى أنه يمكن تطبيق قانون الدولة التي ينتمي إليها الشخص بجنسيته، على اعتبار أن الأمر يتصل بشخصية الفرد التي تتعلق به البيانات والمعلومات. غير أن هناك اتجاها يميل إلى تطبيق قانون الدولة التي يوجد بها مركز المؤسسة التي قامت بمعالجة البيانات إلكترونيا[30].

2- الاعتداء على حقوق الملكية الفكرية: إن حقوق الملكية الفكرية من الحقوق المالية المعنوية، كحق المؤلف على أفكاره وحق الموسيقي على لحنه وحق المخترع على اختراعه، وحق التاجر على محله وحق صاحب العلامة التجارية المسجلة باسمه على هذه العلامة[31].

وتعد النزاعات المتعلقة بالاعتداء على حقوق الملكية الفكرية من أكثر النزاعات التي تثيرها الشبكة الدولية للاتصالات "الإنترنت"[32]، كاستخدام بعض المواقع لبعض الحقوق الأدبية دون إذن أصحابها كموقع نابستير NAPSTER الذي كان يسمح بتصفح مواقع المشتركين والاستماع للأغاني الحديثة المسجلة لدى الأعضاء

دون مقابل وفي ذات الوقت دون ترخيص من أصحاب الحقوق الأدبية عليها. كذلك هو عند استنساخ البعض لبرامج كمبيوتر دون ترخيص من خلال الشبكة[33].

وهنا يثور التساؤل، وفقا لأي قانون يكون للمضرور الحصول على التعويض عن الاعتداء على حقوقه المالية والأدبية؟

لا يوجد اتفاق حول القانون الواجب التطبيق في هذه الحالة، فيقول البعض بتطبيق قانون مكان تحميل المادة المعتدى عليها، في حين يميل البعض الآخر إلى تطبيق قانون الدولة التي تم فيها استدعاء أو تفريغ المادة المعتدى عليها[34].

غير أن هذه الآراء وكل ما سبق وأن تم عرضه بشأن إعمال قاعدة التنازع التقليدية المقررة على الفعل الضار، تعد كلها منتقدة بالنظر إلى الطابع العابر للحدود لنشاط شبكة الإنترنت.

المطلب الثاني

الانتقادات الموجهة لتطبيق منهج قاعدة التنازع على نزاعات المعاملات الإلكترونية

لقي تطبيق منهج قاعدة التنازع كوسيلة لحل مشكلة القانون الواجب التطبيق على النزاعات الإلكترونية جملة من الانتقادات، لعل أهمها أن هذه النزاعات متولدة عن معاملات تمت عبر شبكة الإنترنت، التي لا تعترف بالحدود الجغرافية بين الدول وهي بالتالي تتنافى مع أسباب وجود القانون الدولي الخاص. (الفرع الأول) ومن ثم تعين إيجاد منهج آخر لحل مشكل القانون الواجب التطبيق على النزاع الإلكتروني. (الفرع الثاني)

الفرع الأول

الإنترنت تتنافى وسبب وجود القانون الدولي الخاص

إن التعامل عبر شبكة الإنترنت يتم في عالم افتراضي لا يعترف بالحدود السياسية (ثانيا) التي تعد أصل وجود القانون الدولي الخاص (أولا)

أولا – ظاهرة الحدود السياسية أصل القانون الدولي الخاص: استقر فقه القانون الدولي الخاص على أن هذا القانون يدين بوجوده إلى ظاهرة الحدود السياسية التي تفصل بين الدول أعضاء الجماعة الدولية، إذ أن هذه الحدود تشكل عقبة قانونية في سبيل نشأة ونمو علاقات الأفراد في الدول المختلفة وهي عقبة دعت إلى وجود القانون الدولي الخاص لتذليلها.

ذلك أنه إذا تمت علاقة قانونية عبر الحدود، أي بين أفراد من دول مختلفة فيكون هناك ادعاء من قبل قانون أكثر من دولة الاختصاص بتنظيمها، وهو ما سمي بتنازع القوانين.

وعليه ولدت الحاجة إلى قواعد القانون الدولي الخاص كي تفض هذا التنازع عن طريق اختيار القانون الملائم والمناسب من بين القوانين المتنازعة في الدول التي تتصل بها العلاقة أو الرابطة القانونية التي نشأت عبر الحدود كي يتولى تنظيمها وفض الخلاف بشأنها[35].

ثانيا – العالم الافتراضي لشبكة الإنترنت لا يعترف بالحدود السياسية:

كما أسلفنا بيانه، فإن القانون الدولي الخاص يدين بوجوده لظاهرة الحدود السياسية، ومن ثم فإنه من غير الإمكان الاعتماد على منهج التنازع لحل مشكلة القانون الواجب التطبيق على المعاملات الإلكترونية وبصفة خاصة المعاملات الإلكترونية التي تتم عبر الشبكة الدولية الإنترنت، إذ أن هذه الأخيرة لا تعترف بالحدود السياسية بين الدول، فمجتمع الإنترنت هو مجتمع افتراضي له أشخاصه وأدواته وبطبيعته ليس له حدود سياسية جغرافية وتتعارض مع فكرة الإقليم والجغرافيا[36].

إن مناهج القانون الدولي الخاص التي تقوم على مرتكزات مكانية وجغرافية لا تتلاءم وطبيعة المعاملات والعمليات التي تتم عبر شبكة الإنترنت، وتسبح في فضاء افتراضي ليس له روابط أو صلات مكانية أرضية[37].

الفرع الثاني

الحاجة إلى قانون موضوعي لا إسنادي لحكم المعاملات الإلكترونية

أمام قصور وعجز منهج قواعد الإسناد عن حل مشكل القانون الواجب التطبيق على النزاعات الإلكترونية الراجع إلى عدم فاعلية هذه القواعد (أولا)، ظهرت الحاجة إلى إيجاد قانون موضوعي لا إسنادي لتحديد القانون الواجب التطبيق. (ثانيا).

أولا – عدم فعالية قواعد الإسناد: تعد قواعد منهج التنازع أو كما تسمى قواعد الإسناد، قواعد غير مباشرة في حل مشكلة القانون الواجب التطبيق على العلاقة القانونية المنطوية على عنصر أجنبي، فهذه القواعد لا تقدم حلولا مباشرة للمسالة محل النزاع، فهي تعتمد على الطابع الآلي في اختيار القانون الواجب التطبيق بغض النظر عن كون هذا الاختيار يحقق العدالة للقضية محل النزاع من عدمه بحكم أنها قواعد آلية تنتهي وظيفتها بإرشاد القاضي إلى القانون الواجب التطبيق دون التنبؤ مسبقا بهذا القانون أو معرفته[38].

كما أن قاعدة الإسناد التي تحدد القانون الواجب التطبيق، إنما تحدد قانونا داخليا لدولة ما، من بين القوانين المتزاحمة، لحكم العلاقة محل النزاع، وهذا القانون الذي سيحكم نزاع ناتج عن علاقة ذات طابع دولي، هو قانون موضوع أصلا لحكم وتنظيم العلاقات الوطنية الداخلية، في حين أن الأقرب أن تحكم بقواعد قانونية من الطبيعة ذاتها، أي قواعد دولية [39].

وعليه، فإن منهج التنازع عاجز عن حل مشكل القانون الواجب التطبيق على النزاعات الناتجة عن العلاقات الخاصة الدولية، لأنه لا يراعي خصوصيتها، ولا التطور الذي تشهده لاسيما ظهور ما يسمى بالنزاعات الإلكترونية.

ثانيا– نحو إيجاد قانون موضوعي مادي للمعاملات الإلكترونية: أمام عجز منهج قواعد تنازع القوانين عن حل مشكلة القانون الواجب التطبيق على النزاعات الناشئة عن المعاملات الإلكترونية، ظهرت دعوات إلى إيجاد قانون موضوعي

مادي يحكم المعاملات الإلكترونية، على غرار الدعوات التي أدت إلى ميلاد منهج القواعد المادية الموضوعية الذي يحكم المراكز القانونية الناشئة في إطار التجارة الدولية، وهي مراكز لم يعد من المناسب في ظل تطورها المعاصر أن تبقى خاضعة للقوانين الداخلية التي تشير قواعد التنازع التقليدية إلى اختصاصها[40]. هذه القواعد المتكونة من عادات وأعراف وممارسات ذات نشأة تلقائية أو قواعد تشريعية وطنية أو من أصل اتفاقي دولي، وتكون واجبة التطبيق مباشرة بمجرد ثبوت دخول المنازعة في مجال تطبيقها ودون حاجة إلى إعمال قاعدة التنازع[41].

وعلى هذا الأساس نتساءل عن ماهية هذا المنهج الموضوعي، وكيفية إعماله لحل النزاعات الناشئة عن المعاملات الإلكترونية؟

المبحث الثاني

النزاعات الإلكترونية ومنهج القواعد المادية الموضوعية كحل لمشكلة القانون الواجب التطبيق

أمام تعذر إعمال منهج التنازع التقليدي في مجال المعاملات الإلكترونية بالنظر لصعوبة توطين هذه العلاقات أو تركيزها مكانيا وفقا لمقتضيات هذا المنهج، أصبح من الطبيعي أن يفسح المجال لمنهج آخر هو منهج القواعد المادية الدولية الموضوعة خصيصا لحكم المعاملات الإلكترونية، أو بعبارة أخرى ظهرت الضرورة الملحة إلى قانون موضوعي الكتروني دولي. (المطلب الأول)

لكن لم يسلم هذا المنهج بدوره من الانتقادات، ترجع بالأساس إلى كون هذا القانون حديث النشأة ولم يكتمل بنيانه القانوني بعد وهوعاجز عن تقديم حلول مناسبة لبعض المشكلات. (المطلب الثاني)

المطلب الأول

ضرورة القانون الموضوعي الإلكتروني الدولي للمعاملات الإلكترونية

للوقوف على ماهية هذا القانون الموضوعي الإلكتروني، فمن الأهمية تحديد مفهومه (الفرع الأول)، من ثم ماهي مصادره؟ (الفرع الثاني).

الفرع الأول

مفهوم القانون الموضوعي الإلكتروني

لتحديد مفهوم القانون الموضوعي الإلكتروني، ينبغي التطرق إلى تعريفه (أولا) من ثم تحديد خصائصه، (ثانيا).

أولا- تعريف القانون الموضوعي الإلكتروني: يمكن تعريف القانون الموضوعي أو المادي عموما بأنه ذلك القانون الذي يضع مباشرة تنظيما موضوعيا خاصا ومستقلا عن حلول القوانين الوطنية للمعاملات القانونية بالنظر إلى صفتها الدولية[42]، وفي مجال المعاملات الإلكترونية، فيمكن القول أن القانون الموضوعي الإلكتروني الدولي هو نظير للقانون الموضوعي للتجارة الدولية. ويتشكل من مجموعة من العادات والممارسات المقبولة التي نشأت واستقرت في المجتمع الافتراضي للإنترنت وطورتها المحاكم ومستخدمي الشبكة وحكومات الدول في مجال تكنولوجيا الاتصال والمعلومات، وهكذا يتميز هذا القانون بتلقائية نشأته مما يتيح له أن يتطور باستمرار مع تطور حاجات المتعاملين عبر الشبكة الدولية للاتصالات كما تسمح له هذه التلقائية التوافق مع توقعات المتعاملين مع الشبكة لأنه ينشأ من خلال ممارساتهم وعاداتهم المقبولة[43].

وجدير بالملاحظة إلى أنه على مستوى الفقه تعددت المصطلحات المستخدمة للتعبير عن القواعد التي تحكم المعاملات الإلكترونية لاسيما تلك التي تتم عبر الشبكة الدولية للاتصالات، ومن أمثلة هذه المصطلحات: مصطلح القانون الإلكتروني، قانون المعلوماتية، القانون الافتراضي، القانون الرقمي، قانون الإنترنت، قانون الاتصالات، قانون الفضاء الافتراضي والقانون الموضوعي للإنترنت. بينما يميل اتجاه آخر إلى تسميتها على غرار القواعد المادية للتجارة الدولية فيطلق عليها مصطلح القانون الطائفي، القانون التجاري عبر الدول، قانون فوق الدول، قانون التجارة الجديد وقانون التجارة الرقمي، بينما سماه البعض الآخر بالقواعد المادية للتجارة الإلكترونية. ومها كانت التسمية التي تطلق عليه، فهو

عبارة عن مجموعة من القواعد التلقائية ذات الطبيعة الموضوعية الخاصة بالروابط القانونية التي تتم عبر الشبكات الإلكترونية[44]. أي قواعد أوجدها المتعاقدون وساهمت المنظمات الدولية والإقليمية وبعض القوانين الوطنية الخاصة في تكريسها والاعتراف بها، لتكون قانونا خاصا وجد أساسا لحكم العلاقات العقدية المبرمة عبر الإنترنت عن طريق مدّ المتعاملين بحلول مباشرة على عكس قواعد الإسناد الحيادية غير المباشرة التي تكتفي بتعيين القانون الواجب التطبيق[45].

ثانيا – خصائص القانون الموضوعي الإلكتروني: يتميز هذا القانون بالخصائص التالية:

1– **قانون طائفي ونوعي:** إن المجتمع الدولي للمعاملات الإلكترونية له معطياته ومشكلاته الذاتية التي تستوجب حلولا تتوافق مع ذاتيته، وبالتالي تقتضي قواعد تخاطب فئة معينة من الأشخاص متعاملي الإنترنت وعليه فهو قانون طائفي بالنسبة إلى المخاطبين بأحكامه، فضلا عن ذلك فهو قانون نوعي، حيث أن قواعده وأحكامه لا تنظم إلا نوعا معينا من المعاملات والمسائل. ولهذا القانون الطائفي النوعي نظام مؤسسي مرتب ذاتيا له أجهزته وأدواته فالي جانب قواعده القانونية الخاصة له قضاته و عدالته الافتراضية[46].

2– **قانون تلقائي النشأة:** تتميز قواعد القانون الدولي الإلكتروني بأنها قواعد تلقائية أو ذاتية نابعة من مجتمع ذاتي، أي لا تقوم على تنظيمها جهة رسمية ولا تأتي عن طريق المرور بالإجراءات الشكلية اللازمة لسن القوانين الوضعية ومن ثم تبدو ملائمتها لطبيعة التعاملات عبر الشبكة [47].

3– **قانون دولي موضوعي أو مادي:** من خصائص القانون الدولي الإلكتروني بأنه قانون دولي، ويتأتى الطابع الدولي لهذا القانون من طبيعة المعاملات التي يحكمها، التي تتم عبر شبكة دولية للاتصالات "الإنترنت"، لأن أطراف هذه المعاملات وهم بصدد إنجاز معاملاتهم يتواجدون ماديا في دول مختلفة، بل يمكن القول بأن معيار الدولية لهذه المعاملات يتحقق حتى وان كانت المعاملة بين

وطنيين مقيمين في دولة واحدة، إذ أن التعامل عبر الشبكة يتدخل فيه أشخاص كمزود الخدمة، أو معالج البيانات أو ناقل المعلومات[48]. فضلا عن دولية هذا القانون فهو موضوعي يقدم الحل المادي للمسألة محل النزاع مباشرة ولا يحيل إلى غيره لاستمداد ذلك الحل كما تفعل قواعد الإسناد[49].

الفرع الثاني

مصادر القانون الموضوعي الإلكتروني

تتمثل مصادر القانون الموضوعي الإلكتروني في القواعد الموضوعية ذات النشأة التلقائية (أولا)، وفي القواعد الموضوعية ذات النشأة التنظيمية (ثانيا).

أولا– القواعد الموضوعية ذات النشأة التلقائية: تتمثل هذه القواعد في:

1– **الممارسات التعاقدية:** تعتبر الممارسات التعاقدية من المصادر المهمة للقانون الموضوعي الإلكتروني. وهذه العقود هي على نوعين: الأول يتمثل في مجموعة العقود الخاصة بالاشتراك في شبكة الإنترنت المبرمة بين الراغبين في استخدام الشبكة وبين الشركات التي تقدم خدمة الاشتراك، أما الثاني فهو مجموعة العقود التي تبرم بين مقدم المادة المراد إدخالها وتحميلها على شبكة الإنترنت وبين مقدم خدمة الموقع الذي ستبث تلك المادة عليه[50].

2– **الأعراف والعادات المستقرة:** لقد عرفت العادات والأعراف المستقرة بأنها "مجموعة الأعراف والعادات والقواعد غير الصادرة عن سلطة رسمية والتي تولد بشكل عفوي من قبل فئة أو جماعة معينة تطبقها وتعتبرها ملزمة، ثم تمتد تدريجيا مع الوقت وتتوسع رقعة انتشارها لتلقي في مرحلة أولى قبولا واعترافا من قبل المعنيين بها، وفي مرحلة ثانية من قبل المحاكم حتى تكتسب بنتيجة هذا القبول والاعتراف قيمة قانونية ملزمة."[51].

ثانيا: القواعد الموضوعية ذات النشأة التنظيمية: كما تقدم بيانه، تمثل القواعد المادية الإلكترونية أحد أهم المصادر الدولية للقواعد الإلكترونية التي تشكلت خارج الإطار الوطني، والتي من خلالها يمكن إيجاد الحلول الذاتية للمشكلات الخاصة

بالإنترنت والتجارة الإلكترونية. إلا أنه في المقابل توجد إلى جانبها العديد من المصادر التنظيمية النابعة من أعمال المنظمات الدولية والإقليمية المعنية بالإنترنت والتجارة الإلكترونية. قد تجد هذه القواعد مصدرها في الاتفاقيات الدولية والتوصيات الدولية الأساسية وتقنينات السلوك[52].

المطلب الثاني

تقييم القانون الموضوعي الإلكتروني الدولي للمعاملات الإلكترونية

أثار القانون الموضوعي الإلكتروني العديد من التساؤلات لعل أبرزها، هي مدى اتصافه بصفة النظام القانوني (الفرع الأول)، فضلا عن ذلك يعاب عليه إنه يعد قاصرا عن تقديم حلول لكثير من المشكلات في مجال المعاملات الإلكترونية (الفرع الثاني).

الفرع الأول

مدى تمتع القانون الموضوعي الإلكتروني بصفة النظام القانوني

اختلف الفقه بين مؤيد ومعارض لفكرة تكوين قواعد القانون الدولي الإلكتروني لنظام قانوني، فقد ذهب البعض إلى أنه يصعب القول بأن تلك القواعد تشكل نظاما قانونيا (أولا) في حين قرر البعض الآخر بأن تلك القواعد تشكل نظاما قانونيا بالمعنى الدقيق لهذا الاصطلاح (ثانيا).

أولا- نفي صفة النظام القانوني عن القانون الموضوعي الإلكتروني:

يذهب أنصار هذا الاتجاه إلى نفي صفة النظام القانوني عن ذلك القانون الموضوعي الإلكتروني مستندين في ذلك إلى عدة حجج:

1- إن صفة النظام القانوني لا تتوافر إلا حيث نكون بصدد جماعة متماسكة ومنتظمة بشكل كاف، وهو فرض يفرضه الواقع العملي عبر شبكة الإنترنت. فجماعة الإنترنت تضم أشخاصا ينتمون إلى دول وأنظمة قانونية متباينة، وهم في الغالب لايعرفون بعضهم البعض، ولا يوجد بينهم رابط اجتماعي سابق على رباط

العمل، ولا تجمعهم ثقافة واحدة، فهي جماعة تفتقد إلى الوحدة والتماسك اللازمين لأي نظام قانوني[53].

فمجتمع الإنترنت مجتمع غير متجانس وتتعارض مصالح أشخاصه، بل حتى الدول لن تكون متعاونة في هذا الشأن، فليس لديها الاستعداد لترك المنازعات التي يكون مواطنوها أطرافا فيها كي يحكمها ذلك القانون. كما أن المصالح الاقتصادية والسياسية لكل دولة سوف تعوق كل محاولة لوجود واكتمال مثل هذا القانون الموضوعي[54].

2- إن قواعد هذا القانون تفتقد لعنصر الإلزام لعدم اقترانها بجزاء توقعه سلطة عامة عند مخالفتها، ويعتمد تطبيقها على إرادة الأطراف[55].

ثانيا- الاعتراف بصفة النظام القانوني للقانون الموضوعي الإلكتروني:

خلافا للاتجاه السابق، يذهب أنصار هذا الاتجاه إلى أن قواعد القانون الموضوعي الإلكتروني تشكل نظام قانوني موضوعي ذاتي خاص بالعمليات التي تتم عبر الإنترنت، وهو نظير للقانون الموضوعي للتجارة الدولية، ويتشكل من مجموعة من العادات والممارسات المقبولة التي نشأت واستقرت في المجتمع الافتراضي للانترنت، وطورتها المحاكم ومستخدمو الشبكة، وحكومات الدول في مجال تكنولوجيا الاتصال والمعلومات. فهو مجتمع تلقائي النشأة، وجد ليتلاءم مع حاجات مجتمع قوامه السرعة في التعامل، والبيانات الرقمية التي تتم بها المعاملات والصفقات عبر شاشات أجهزة الحواسب الآلية، ويتوافق مع توقعات أطراف تلك العلاقة[56].

الفرع الثاني

نقص وقصور قواعد القانون الموضوعي الإلكتروني

إذا كنا قد انتهينا أعلاه، إلى أن قواعد القانون الموضوعي الإلكتروني تشكل نظاما قانونيا مستقلا، إلا أنها ونظرا لحداثتها تبقى قاصرة على حكم جميع

المعاملات الكترونية (أولا)، فستظل الحاجة ماسة إلى القواعد التقليدية وبالتالي إعمال المنهج التقليدي لتنازع القوانين (ثانيا).

أولا-عدم كفاية القواعد الموضوعية للقانون الدولي الإلكتروني: للبحث عن مدى كفاية قواعد القانون الموضوعي ينبغي تحليل مصادر ومكونات هذه القواعد فبالعودة إلى الاتفاقيات الدولية التي تعد مصدرا من مصادر القانون الموضوعي الإلكتروني، يتضح أن هناك تناقضات كثيرة فيما بين هذه الاتفاقيات سواء في شان إجراءات ووسائل الإثبات أو بخصوص تنقيح أو تعديل تلك الاتفاقيات، مما يترتب عليه صعوبة تطبيقها في مجال المعاملات الإلكترونية لاسيما التجارة الإلكترونية[57].

كما أن قواعد هذا القانون لا يمكن أن تكون نظاما قانونيا كاملا ومستقلا قادرا على تقديم الحلول لجميع مشكلات المعاملات الإلكترونية التي يمكن أن تثور، وهذا راجع على وجه الخصوص لكونها لا تزال في بدايتها الأولى، أي في طور التكوين[58].

ثانيا- بقاء الحاجة إلى إعمال منهج قاعدة التنازع إلى جانب القواعد الموضوعية للقانون الإلكتروني: على الرغم من مساهمة القانون الموضوعي الإلكتروني في إعطاء حلول لمشكلات مطروحة على مستوى المعاملات الإلكترونية، حلولا لا يمكن أن تقدمها القوانين الوطنية التي كرست لتتلاءم مع المعاملات التقليدية، إلا انه تبقى هذه القواعد حديثة النشأة وفي مرحلة التكوين وعليه تتضمن العديد من الفراغات، مما يعني أن المعاملات الإلكترونية ستظل في حاجة إلى القواعد التقليدية، التي تتضمنها القوانين الوطنية، وعليه ستظل الحاجة ماسة إلى قواعد القانون الدولي الخاص[59].

خاتمة: إن النزاعات الإلكترونية التي تتم عبر الشبكة الدولية للاتصالات "الإنترنت"، تتسم بالطابع الدولي لأنها ناشئة عن معاملات الكترونية دولية. ولا يخفى أن هذا الطابع الدولي من شأنه أن يثير العديد من المشكلات على مستوى

القانون الدولي الخاص، لاسيما مشكلة تحديد القانون الواجب التطبيق على المعاملات محل النزاع.

ولما كان القانون الدولي الخاص يرتكز على منهج أصيل في تحديد القانون الواجب التطبيق ألا وهو منهج قاعدة التنازع، فدرسنا مدى إمكانية إعمال هذا المنهج على هذه المعاملات؟ ليتبين أن هذا التطبيق قد لقي جملة من الانتقادات لعل أهمها أن هذه النزاعات متولدة عن معاملات تمت عبر شبكة الإنترنت، التي لا تعترف بالحدود الجغرافية بين الدول وهي بالتالي تتنافى مع أسباب وجود القانون الدولي الخاص، فمنهج قاعدة التنازع الذي يقوم على مرتكزات مكانية جغرافية لا يلائم طبيعة المعاملات التي تتم عبر شبكة الإنترنت، وتسبح في فضاء افتراضي ليس له روابط مكانية أرضية.

أمام قصور وعجز هذا المنهج عن حل مشكلة القانون الواجب التطبيق على النزاعات الإلكترونية، ظهرت الدعوات إلى معالجة المشكل بانتهاج منهج القواعد المادية الموضوعية. هذا المنهج الذي يقوم على تطبيق القانون الموضوعي الإلكتروني الذي يعد نظيرا للقانون الموضوعي في مجال التجارة الدولية.

هذا القانون لم يسلم بدوره من الانتقادات، لعل أبرزها أنه، قانون حديث النشأة وهو في طور التكوين، وبالتالي قواعده لا تشكل نظاما قانونيا كاملا ومستقلا لحكم المعاملات الإلكترونية ولا يقدم الحلول لعديد من المشكلات.

ومن ثم، وبالنظر إلى خصوصية المعاملات الإلكترونية وحداثة القواعد القانونية الخاصة بها، فمن الضروري لحل مشكل القانون الواجب التطبيق إعمال المنهجين معا، ويكون ذلك بان يبحث القاضي أولا على القاعدة المادية ليطبقها على النزاع المعروض أمامه ذي الطابع الإلكتروني، وإن لم يجدها فما عليه سوى الاستعانة بقواعد الإسناد لتبين له ماهو القانون الواجب التطبيق، ومما لا شك فيه أنه ستواجه القاضي غير قليل من الصعوبات متمثلة فيما سبق ذكره من صعوبات إعمال منهج قاعدة التنازع.

وعليه، وعلى الرغم من تعدد الإمكانات التي يتيحها استخدام شبكات الاتصال الإلكتروني، إلا أن المشاكل أو المسائل القانونية التي يثيرها هذا الاستخدام لم تحظ بالاهتمام الكافي. ويتعين أن يكون واضحا أن ازدهار المعاملات الإلكترونية يتوقف على جريانها في وسط قانوني يكفل الأمن للمعاملات ويحمي حقوق وحريات أطرافها ويحيط المصالح المتعلقة بالنظام العام، سواء الداخلي أو الدولي، بسياج متين من الحماية.

1- ومن التشريعات الوطنية المقارنة التي كرست هذه القاعدة، نذكر على سبيل المثال القانون المدني المصري، كما تبنتها أيضا العديد من الاتفاقيات الدولية، منها اتفاقية روما لعام 1980 بشأن القانون الواجب التطبيق على الالتزامات التعاقدية فيما بين دول السوق الأوروبية المشتركة (الاتحاد الأوربي حاليا).

- انظر: أحمد عبد الكريم سلامة، "الإنترنت والقانون الدولي الخاص: فراق أم تلاق"، في: *بحوث مؤتمر القانون والكمبيوتر والإنترنت*، المجلد الأول، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص. 85.

2- تعد الإرادة أساس التصرف القانوني، فهي التي تنشئه وهي التي تحدد آثاره، وهذا ما يعبر عنه الفقه بمبدأ سلطان الإرادة.

- حول نشأة المبدأ وتطوره، راجع: عبد الرازق السنهوري، الوسيط في شرح القانون المدني الجزء الأول: مصادر الإلتزام، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، 1998.

3- أمر رقم 75-58، مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، ج. ر. ج. ج. عدد 78، صادر بتاريخ ــ 30 سبتمبر 1975، معدل ومتمم.

4- تفصيلا حول هذه الاتجاهات راجع:

- صالح المنزلاوي، *القانون الواجب التطبيق على عقود التجارة الالكترونية*، دار الجامعة الجديدة، الإسكندرية، 2006، ص ص. 269 – 275.

5- ناصر حمودي، *النظام القانوني لعقد البيع الدولي الالكتروني المبرم عبر الإنترنت*، رسالة لنيل شهادة الدكتوراه في العلــوم، التخصص: القــانون، جــامعة مولــود معمري، تيزي وزو 2009، ص. 416.

6- المرجع نفسه، الصفحة نفسها.

7- صالح المنزلاوي، مرجع سابق، ص ص. 279-281.

8- غالب علي الداودي، حسن محمد الهداوي، القانون الدولي الخاص، الجزء الأول، د. د. ن، د. ت. ن.، ص. 130.

9 - نقلا عن: سمية بن غرابي، *عقود التجارة الالكترونية ومنهج تنازع القوانين*، مذكرة لنيل درجة الماجستير في القانون، فرع قانون التعاون الدولي، جامعة مولود معمري، تيزي-وزو 2009، ص. 99.

10- أحمد الهواري، "عقود التجارة الالكترونية في القانون الدولي الخاص"، *مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون*، المجلد الرابع، غرفة تجارة وصناعة دبي، 10-12 مايو، 2003، ص. 1654.

11- ومثال ذلك: العقد النموذجي للتجارة الإلكترونية الذي وضعته غرفة التجارة والصناعة بباريس في 30 أفريل 1998 ليحكم المعاملات التي تتم بين المهنيين والمستهلكين

- انظر: صالح المنزلاوي، مرجع سابق، ص ص. 269 - 275.

12- انظر، أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي (الالكتروني، السياحي، البيئي)* دار النهضة العربية، القاهرة، ص. 85.

13- ومن ذلك القرائن المستمدة من المحكمة التي اتفق على تخويلها الاختصاص بمنازعات العقد وهي قرينة مهمة تفيد أن من يختار القاضي يختار قانونه، ومن القرائن أيضا العملة التي يتم الدفع بها، مكان الوفاء ولغة العقد... الخ.

14- صالح المنزلاوي، مرجع سابق، ص. 286.

15- نقلا عن: أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي...*، مرجع سابق، ص. 85.

16- انظر، بلقاسم أعراب، *القانون الدولي الخاص الجزائري (تنازع القوانين)*، الزيتونة للإعلام والنشر، د. ت.، ص. 279.

17- ناصر حمودي، مرجع سابق، ص 421.

18- غالب علي الداودي، حسن محمد الهداوي، مرجع سابق، ص 138.

19- حسن الهداوي، *القانون الدولي الخاص: تنازع القوانين، المبادئ العامة والحلول الوضعية في القانون الأردني، دراسة مقارنة*، مكتبة دار الثقافة للنشر والتوزيع، عمان، 1997، ص ص. 158-160.

20- المرجع نفسه، ص. 160.

21- علي الداودي، حسن محمد الهداوي، مرجع سابق، ص. 139.

22- يوسف العلي، "مدى صلاحية قواعد تنازع القوانين لحكم التعاملات التي تتم على شبكة الإنترنت، دراسة في القانون الدولي الخاص الكويتي"، ص. 12. /www.arablawinfo.com

23- محمد محمود علي، *مدى تأثير التجارة الإلكترونية في تنازع القوانين ذي الطابع الدولي*، دار النهضة العربية، القاهرة، 2013، ص.421.

24- أحمد عبد الكريم سلامة، "الإنترنت والقانون الدولي الخاص...، مرجع سابق، ص. 86.

25- ولقد أخذت بعض التشريعات المقارنة بهذا الموقف، منها القانون الدولي الخاص الإنجليزي لعام 1995.

- انظر، محمد محمود علي، مرجع سابق، ص 422.

26 -المرجع نفسه، ص 423.

27 – Éric A Caprioli, *Règlement des litiges internationaux et droit applicable dans le commerce électronique, (Tribunal compétent, loi applicable, Droit pénal international, Arbitrage en ligne)*, LITEC, Édition du juris – classeur, PARIS, 2002 op cit., p.30.

28 – عبد الفتاح بيومي حجازي، *التجارة الالكترونية وحمايتها القانونية*، دار الفكر الجامعي الإسكندرية، 2004، ص. 80.

29- أحمد عبد الكريم سلامة، " الإنترنت والقانون الدولي الخاص...، مرجع سابق، ص. 86.

30- وهذا ما أخذ به التوجيه الأروبي رقم 95-46 المؤرخ في 24 /1995/10 الخاص بحماية الأشخاص الطبيعيين بالنسبة للمعالجة الآلية للبيانات ذات الطابع الشخصي وحرية تداول ونقل البيانات.

- نقلا عن المرجع نفسه، ص. 88.

31- عبد الفتاح بيومي حجازي، مرجع سابق، ص. 13.

32- أيوب بولين أنطونيوس، مرجع سابق، ص 46.

33- يوسف العلي، مرجع سابق، ص. 28.

34- أحمد عبد الكريم سلامة، "الإنترنت والقانون الدولي الخاص...، مرجع سابق، مرجع سابق ص ص. 91-94.

35 - أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي*...، مرجع سابق، ص. 35 وما بعدها.

36- ناصر حمودي، مرجع *سابق*، ص. 428.

37- أحمد الهواري، مرجع سابق، ص. 1661.

38 - عمر بلمامي، "نظرة تأملية حول مستقبل قواعد الإسناد في ظل عولمة القانون"، *المجلة الجزائرية للعلوم القانونية الاقتصادية والسياسية*، عدد 04، 2007، ص. 153.

39 - سمية بن غرابي، مرجع سابق، ص. 129.

40- صالح المنزلاوي، مرجع سابق، ص. 01.

41- أحمد عبد الكريم سلامة، "خمسون عاما خلت من عمر قواعد التنازع المصرية: الحاجة إلى التعديل أو الاستقلال"، *المجلة المصرية للقانون الدولي*، المجلد الثالث والخمسون، 1997، ص. 22.

42- أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي*...، مرجع سابق، ص. 47.

43- أحمد الهواري، مرجع سابق، ص. 1662.

44 - صالح المنزلاوي، مرجع سابق، ص. 110وما بعدها.

45 - ناصر حمودي، مرجع سابق، ص. 434.

46- أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي*...، مرجع سابق، ص ص.55-57.

47 - صالح المنزلاوي، مرجع سابق، ص ص. 183- 184.

48 - عزت محمد علي البحيري، "القانون الواجب التطبيق على المعاملات الالكترونية"، *مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون*، المجلد الرابع، غرفة تجارة وصناعة دبي 10-12 مايو، 2003، ص 1669.

49- أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي...*، مرجع سابق، ص ص. 59- 61.

50- المرجع نفسه، ص. 48.

51 - أشير إلى هذا التعريف لدى: حمودي ناصر، مرجع سابق، ص 436.

52- صالح المنزلاوي، مرجع سابق، ص. 118.

53- المرجع نفسه، ص. 201.

54- أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي...*، مرجع سابق، ص. 63.

55- أحمد الهواري، مرجع سابق، ص. 1664.

56- المرجع نفسه، ص. 1662.

57- صالح المنزلاوي، مرجع سابق، ص. 226.

58- أحمد الهواري، مرجع سابق، ص. 1664.

59- أحمد عبد الكريم سلامة، *القانون الدولي الخاص النوعي...*، مرجع سابق، ص. 66.

الطّبيعة القانونيّة للجريمة الإلكترونيّة وسبل الحدّ منها

الأستاذة المحامية كاهنة محيوت

جامعة مولود معمري، تيزي – وزّو

– **مقدَّمة:** لقد فطر الله الإنسان منذ الأزل على ارتكاب الجرائم، فأوّل جريمة مرتكبة في هذا الوجود هي التي وقت بين ابني آدم عليه السّلام، قابيل وهابيل؛ حيث قتل الأوّل الثّانيّ لأسباب تاريخيّة معروفة لدى الجميع، ومهما تكن الأسباب التي تدفع الإنسان إلى ارتكاب الجرائم، وأيّا تكن الدّوافع الشّخصيّة الدّفينة في نفسه الأمّارة بالسّوء والتي تشير عليه بإلحاق الأذى بغيره، نقول إنّ حجم الخسائر المعنويّة والنّفسيّة التي تصيب الضّحيّة لا تعوّض بثمن؛ حيث إنّ الجريمة تحمل معاني القهر والفساد على الفرد وتمتدّ إلى المجتمع بأسره، وبالتّالي سيعمّ الخراب في الكون.

إن التّطوّر الهائل للشّبكة العنكبوتيّة أدّى إلى زيادة عدد مستخدميه في كلّ أقطار العالم من جميع الفئات والأعمار والأجناس، وهو بذلك يكون قد محا معالم وحدودًا وأصبح الفرد يصول ويجول فيها بلا منازع أو رقيب ينهاه أو يزجره في ما يفعل داخلها، من أفعال أو أقوال، وهذا ما أسهم في ظهور الجرائم الإلكترونية على تعدّد أشكالها وألوانها، تلك التي دقّت ناقوس الخطر وجرس الإنذار لتنبّئ بتدهور الحالة التي وصل إليها الأفراد المجرمون من مستخدمي الإنترنيت، ناهيك عن مئات الجرائم التي قد ارتكبت فعلا ولم يعرف بعد الفاعل، سوى أنّ هناك مئات الضّحايا وبذلك ظهر ما يسمّى بمجرم الكمبيوتر.

ولقد ثار الجدل نتيجة توسع مجال الجريمة وتعدّد أشكالها، حول ماهية الجريمة الإلكترونيّة، وبالتّالي صاحب التّطوّرُ التّقنيّ ظهورَ أشكال من السّلوكيّات التي تهدّد أمن واستقرار المجتمع، وتضرّ بمصالح الأشخاص، الأمر الذي دفع المشرّع في

بعض الدّول إلى تجريمها، وتقرير عقوبات على مرتكبيها، مع العلم أن النّصوص التّشريعيّة تبدو قاصرة في مواجهة هذه الجرائم التي انتشرت بسرعة.

إن الجرائم التي سوف نعالجها من خلال هذه المداخلة هي الجرائم التي ترتبط بالشّبكة العنكبوتيّة، المسمّاة بالجريمة الإلكترونيّة أو جريمة الكمبيوتر، وبالتّالي سوف نتعرّض بالدّراسة والتّحليل إلى إبراز النُّقاط المهمّة المتعلّقة بهذه الجريمة من جانبها القانونيّ، مع الإشارة إلى بعض الحلول المناسبة لها، والّتي تتمحور حولها الإشكاليّة العامّة التّالية: **ما هي الطبيعة القانونية للجريمة الإلكترونية، وما سبل الحد منها؟**

1- **تعريف القانون:** يمكن تعريف مصطلح **قانون** من جانبين: الجانب اللّغويّ والاصطلاحيّ المرتبط بالقضاء.

أ/ **الأصل اللّغويّ لكلمة قانون:** "يرجع أصل كلمة قانون إلى اللّغة اليونانيّة فهي معرّبة أُخذت من الكلمة اليونانيّة kanun أو من الكلمة اللاّتينيّة kanon ومعناها العصا المستقيمة"[1]؛ ومعنى ذلك أنّ مصطلح قانون يحمل معنى ساميا يهدف إلى الإصلاح والتّرقية وتوقيع العقوبة على مخالف القواعد القانونيّة المسَنّة في المجتمع؛ إذ إنّه يدلّ في معناه اللّغويّ على العصا المستقيمة التي لا تحمل اعوجاجا، وبالتّالي دلالته دائما على الطّريق الصّحيحة. هذا بغضّ النّظر على أنّ هذا المصطلح يرادفه باللّغة الفرنسيّة كلمة Droit، وباللّغة الإنجليزيّة كلمة Law وهي كلّها ذات معنى واحد.

ب/ **المعنى الاصطلاحيّ لكلمة قانون:** تدلّ كلمة قانون في معناها العامّ على مجموعة القواعد القانونيّة العامّة والمجرّدة والملزمة للأفراد Règles générales, abstraites et obligatoires المكتوبة أو غير المكتوبة المستمدّة من المصادر المختلفة كالتّشريع والشّريعة الإسلاميّة والعرف، وغيرها محدّد في القانون الجزائري على وجه الخصوص، والقانون الدّوليّ على وجه العموم؛ وبالتّالي ضرورة احترامها من طرف الجميع؛ لأنّها تنظّم حياتهم وسلوكيّاتهم في المجتمع، بغضّ النّظر عن اختلاف المكان والزّمان.

2- تعريف الجريمة: "الجريمة لغة مشتقّة من فعل جرم على وزن ضرب والتي تعني الذّنب واكتساب الإثم، أمّا اصطلاحا، فنقصد بها إتيان فعل محرّم نهى عنه الشّارع أو ترك فعل مأمور به، ولا يعدّ الفعل أو التّرك جريمة إلاّ إذا تقرّرت عليه عقوبة محدّدة"[2]؛ ومعنى ذلك أنّ المجرم برئ إلى غاية إدانته أو إثبات التّهمة عليه، لقيامه بأفعال أو أقوال ضارّة قد سبق أن وضع لها مشرّع القوانين في الدّولة القواعد ونظّم لها العقوبات المناسبة بحسب درجتها في الضّرر الملحق بالضّحية.

أ/ تعريف الجريمة الإلكترونيّة: "تتكوّن الجريمة الإلكترونيّة أو الافتراضيّة (cyber crimes) من مقطعين هما: الجريمة (crime) والإلكترونيّة (cyber) ويستخدم مصطلح الإلكترونيّة لوصف جزء من الحاسب أو عصر المعلومات والجرائم الإلكترونيّة هي المخالفات التي ترتكب ضدّ الأفراد أو المجموعات من الأفراد بدافع الجريمة، ويقصد بها إيذاء سمعة الضّحيّة، أو إلحاق أذًى مادّيّا أو عقليّا للضّحيّة مباشرا أو غير مباشر، باستخدام شبكات الاتّصالات مثل الإنترنيت (غرف الدّردشة، البريد الإلكترونيّ، الموبايل..)، وتشمل الجريمة الإلكترونيّة أبعد من هذا الوصف لتمتدّ إلى جرائم متّصلة بالهويّة والمتعلّقة بمحتويات الكمبيوتر كلّها"[3]؛ ويدلّ هذا الكلام على أنّ الضّرر الذي تلحقه الجريمة الإلكترونيّة معنويّ ومادّيّ؛ فالضّرر المعنويّ يتمثّل مثلا في كشف المستور عن الضّحيّة كنشر صورها أو تزييفها، أمّا الضّرر المادّيّ فينصبّ على الأشياء المادّيّة كالأموال مثلا وغير ذلك كثير من المجالات التي يستطيع فيها المجرم المعلوماتيّ أن ينفّذ بها جريمته.

ب/ التّعريف الدّوليّ للجريمة الإلكترونيّة: ومن بين التّعريفات التي قيلت حول الجريمة الإلكترونيّة ما يلي:

- "عدد محدود من الأفعال ضدّ السّرّيّة والنّزاهة وتوافر بيانات الكمبيوتر، أو أنظمة تمثّل جوهر الجريمة الإلكترونيّة؛
- أعمال متعلّقة بالكمبيوتر لتحقيق مكاسب شخصيّة أو ماليّة أو ضرر، بما في ذلك أشكال الأفعال المتّصلة بجريمة الهويّة"[4]؛ ومن هذين التّعريفين الدّوليّين

نستنتج أنّهما ينصبّان في التّعريف نفسه المعطى للجريمة الإلكترونيّة التي تقوم بتوفّر أركانها المتمثّلة في الجاني والضّحيّة والضّرر والقصد الجنائيّ.

3- **تعريف الإنترنيت:** هو اختصار لكلمتين انجليزيّتين هما: الأولى: International، والثّانية: Network، ويقصد به شبكة الاتّصالات الدّوليّة العالميّة وهذه الشّبكة تربط كلّ قطر وشبر من العالم حتّى إنّها اليوم قد أصبحت قرية صغيرة. ولعلّ من أهمّ التّعريفات التي قيلت في شأن الإنترنيت ما يلي:

- أنّها شبكة هائلة من أجهزة الكمبيوتر المتّصلة في ما بينها بواسطة خطوط الاتّصالات العالميّة، فهي تمثّل شبكة الشّبكات، حيث تتكوّن من عدد كبير من شبكات الطّلب المتزايدة في أنحاء كبيرة من العالم، فالإنترنيت إذًا هو مجموع شبكات وأجهزة للحاسب الإلكترونيّ التي توجد في مختلف دول العالم، والتي تتّصل ببعضها البعض؛ حيث تجمع بينها أنظمة الاتّصالات الإلكترونيّة التي تستخدم لنقل البيانات، ويمكن لأيّ شخص لديه جهاز كمبيوتر، ولديه اشتراك لدى أحد مقدّمي خدمة الإنترنيت وخطّ تلفونيّ، الدّخول إلى شبكة الإنترنيت.
- وقيل الإنترنيت عبارة عن استغلال متقدّم للحاسب الآليّ، مرتبط من خلال الاتّصالات الدّوليّة مع وجوب توافر تقنيّة خاصّة، وهو يمثّل شبكة ضخمة تتكوّن من عدد كبير من شبكات الحاسب الآليّ المنتشرة عبر أنحاء العالم، والمرتبطة بعضها ببعض بواسطة خطوط الهاتف، أو عن طريق الأقمار الصّناعيّة؛ بحيث يمكن تبادل المعلومات بين المستخدمين عن طريق بروتوكول موحّد يسمّى **بروتوكول تراسل الإنترنيت**[5]؛ وبالتالي يمكن القول إنّ الإنترنيت تقنيّة العصر المتطوّرة جدّا التي تقدّم خدمات هائلة للأشخاص والمؤسّسات في ثوانٍ معدودة مختصرة بذلك المسافات والأزمان، وهذه الشّبكة تشكّلها مجموعة لا متناهية من الأجهزة الإلكترونيّة عبر العالم.

4- **استخدامات الإنترنيت:** إنّ من بين الأغراض الكثيرة التي يستخدَم من أجلها الإنترنيت ما يلي ذكرها:

- **البريد الإلكترونيّ:** من خلاله نستطيع إرسال واستقبال الرّسائل بسرعة مذهلة تقدّر بالثّواني.
- **المحادثات الشّخصيّة:** يمكن من خلالها التّحدّث إلى طرف آخر أو أكثر صوتا وصورة وكتابة.
- **خدمة نقل الملفّات:** نستطيع بواسطته نقل البيانات والمعلومات مهما كان حجمها.
- **خدمة الأرشيف الإلكترونيّ:** حيث نستطيع إنشاء وتثبيت ما نحتاجه من معلومات، والرجوع إليها في أيّ وقت بسرعة مذهلة.
- **خدمة البحث في أيّ شيء نحتاجه من خلال شبكة الإنترنيت العالميّة:** فبواسطتها يمكننا استخراج المعلومات والبرامج والمواقع والسّلع ومواقع التّرفيه والإعلانات عن الوظائف وغيرها ممّا يحتاجه الإنسان.
- **خدمة التّسوّق:** فبواسطة شبكة الإنترنيت نستطيع أن نتنقّل من خلال قارّات العالم لاستعراض المنتجات والسّلع، والتّعرّف على أوصافها وأثمانها وطرق نقلها ودفع ثمنها وغير ذلك.
- **التّحويل الماليّ الإلكترونيّ:** وذلك بين البنوك والشّركات والمقاصّة الماليّة بين البنوك، تماما مثل استعمال البطاقات البنكيّة[6]؛ ومعنى ذلك أنّ هذه الشّبكة العنكبوتيّة الهائلة ذات فوائد جمّة بغضّ النّظر عن بعض المجرمين الذين يستخدمونها لتجسيد نواياهم السّيّئة، فلو نظرنا إلى جانبها الإيجابيّ وجدنا أنّها تصنع العلاقات الاجتماعيّة والثّقافيّة والسّياسيّة والعلميّة بين الأشخاص من مختلف الأعمار والفئات والمستويات، عبر البريد الإلكترونيّ والدّردشات والفايس بوك كما أنّ هذه الشّبكة تقدّم خدمات البحث عن كلّ التّساؤلات في مختلف الميادين وتعطينا أجوبة علميّة موثّقة عنها، بالإضافة إلى الخدمات الأخرى المتعلّقة بالميدان التّجاري، وغيرها كثير من الخدمات التي لا تعدّ ولا تحصى.

إنّ التّطوّر السّريع للشّابكة وكثرة تردّد الأشخاص عليها في كل وقت ومكان قد جعل حجم الجرائم تتزايد نظرًا لمعرفتهم كيفيّة تسييرها واطّلاعهم على كلّ

جديد يستجدّ فيها في ما يتعلّق بالبرامج والخدمات المقدّمة منها، وبالتّالي تزايد نوعيّة وكيفيّة الجرائم الإلكترونيّة المرتكبة عبر الإنترنيت، والتي تضرّ بالأشخاص والممتلكات من كلّ الجوانب: سواء الأخلاقيّة أم الإنسانيّة كالقذف والسّبّ والشّتم وخدش كرامة الإنسان واعتباره، أم الاقتصاديّة كالسّرقة واختلاس الأموال وتحويلها، أم السّياسيّة كالإنصات والتّجسّس، أم الاجتماعيّة كالأفعال غير الأخلاقيّة الضّارة بالفرد والمجتمع، والتي تمس المبادئ، وغيرها كثير.

ويمكن المقارنة بين الجريمة التّقليديّة والجريمة الإلكترونيّة كما يلي[7]:

الجريمة التّقليديّة	الجريمة الإلكترونيّة
الاحتيال	الاحتيال على الشّبكة، الاحتيال بالمزاد الإلكترونيّ
السّطو	القرصنة على الإنترنيت، الحرمان من الخدمة الفيروسات.
جرائم الأطفال الجنسيّة	استمالة الأطفال على النّت، المواقع الإباحيّة.
غسيل الأموال	أنظمة الدّفع على الشّبكة.
السّرقة	جرائم الهويّة وسرقة الملكيّة.

5- الطّبيعة القانونيّة للجريمة الإلكترونيّة: إنّ الجريمة الإلكترونيّة هي حديث السّاعة ونقاش حادّ راهن ظهر مؤخّرًا، وعليه نقول إنّها موضوع جديد بالرّغم من أنّ الإنترنيت تقنيّة غير جديدة علينا ولم تظهر مؤخّرًا، ولذلك نجد أنّ المشرّع الجزائريّ قد تأخّر في وضع الإطار القانونيّ لها، وتحديدها وتنظيمها، فثارت هناك مسألتان:

أ/ المسألة الأولى: "تتعلّق بتصنيف الجرائم الإلكترونيّة انطلاقا من تحديد طبيعة الأفعال المجرّمة المنشأة لها"[8]: ومعنى ذلك أنّ الظاهر يقول بتشابه عدد كبير من الجرائم المرتكبة عبر الإنترنيت بالجرائم العاديّة التي حدّدها القانون ووضع لها نظُمَها وعقوباتها وتكييفها القانونيّ الموجود في قانون العقوبات، مثل جريمة السّرقة وتحويل الأموال والقذف والسّبّ والأفعال الإباحيّة، وبالتّالي تخضع للقواعد نفسها.

ب/ المسألة الثّانية: "تتعلّق بتحديد الاختصاص القضائيّ لنظر جرائم الإنترنيت"[9]: ونقصد بالاختصاص القضائيّ الجهة القضائيّة التي تختصّ بالنّظر في الجريمة الإلكترونيّة المرتكبة، وكذا القانون الواجب التّطبيق على مرتكبيها.

إنّ هذه المسألة في غاية التّعقيد من حيث الجانب القانونيّ؛ فإذا نظرنا إلى الاختصاص المكانيّ، فنجد أن الجريمة الإلكترونيّة لا تعرف مكانا محليّا واحدا؛ لأنّ شبكة الإنترنيت شبكة عالميّة فأيّ محكمة تختصّ بالنّظر في الجريمة؟، بغضّ النّظر على أنّ بعض فقهاء القانون قالوا بإمكانية أن تختص محكمة البلد التي ينتمي إليها الشّخص، ولكن ستثور إشكاليّات عدّة في هذا الصّدد هي: كيف يمكن معرفة جنسيّة الشّخص لمّا يتعلّق الأمر بشبكة التّواصل الاجتماعيّ facebook، حتّى وإن تمكّنّا من معرفة بلد الجاني، فأيّ محكمة تختصّ بالنّظر في الجريمة إذا علمنا بأنّ لكلّ جهة قضائيّة اختصاصها المكاني لا يدخل في اختصاص محكمة أخرى وأقصد بذلك أنّ هنالك دعاوي نرفعها مثلا أمام محكمة دائرة معيّنة لا يصحّ رفعها أمام محكمة دائرة أخرى داخل الولاية الواحدة، وبالتّالي يجب تحديد بدقّة المكان الأصليّ والدّقيق للقرية أو المدينة التي يعيش فيها الجاني، أو مكان وقوع الجريمة.

غير أنّ هذه الإشكاليّة قد جعلت الفقهاء ينقسمون إلى عدّة اتّجاهات:

- "**الاتّجاه الأوّل:** يرى أن تكون المحكمة المختصّة بنظر النّزاع هي محكمة الإقليم الذي وقعت فيه الجريمة، حتّى ولو كان المجرم يحمل جنسيّة دولة أخرى ولكنّ الانتقاد الذي وجّه لهذا الاتّجاه هو أنّه لا يقدّم لنا جوابا مناسبا في حال ارتكاب الجريمة في أكثر من دولة.

- **الاتّجاه الثّانيّ:** جعل المحكمة المختصّة هي محكمة محلّ إقامة المدّعى عليه، وقد أخذت معظم التّشريعات العربيّة بهذا الاتّجاه، بيْد أنّه لم يسْلم من النّقد هو الآخر، لاسيما إذا كان هذا الفعل لا يعدّ جُرما في نظر الدّولة محلّ ارتكابه وبخاصّة أنّ صنفًا راجحًا من الدّول لازال بعيدًا عن السّيطرة على أفعال الاعتداء على حقوق الملكيّة الفكريّة، أو الدّعاية الكاذبة أو المضلّلة.

- **الاتّجاه الثّالث:** يرى أنّ المحكمة المختصّة هي محكمة جنسيّة مرتكب الجريمة، بالرّغم من الجاذبيّة التي يتمتّع بها هذا الاتّجاه، إلاّ أنّ صعب التّجسيد من النّاحية العمليّة، وبخاصّة أنّ الجناة المسؤولين عن الجرائم الإلكترونيّة هم على درجة عالية من العلم والمعرفة والذّكاء، ومن ثمّ فإنّ تقفّي آثارهم قد ظلّ أمرًا مستعسرًا"[11]؛ وبالرّغم من أنّ هذه الاّتجاهات الثّلاثة قد اختلف فيها الفقهاء القانونيّون حول الاختصاص الإقليميّ الذي يجب أن يطبّق فيه القانون، إلاّ أنّ الحلّ الأنسب الذي اقترحته معظم الدّول الصّناعيّة الكبرى في نظر الدّكتور (رابحي أحسن) هو قانون الدّولة التي وقعت فيه الجريمة، بالرّغم من صعوبة ذلك في الواقع العمليّ.

6-تحديد الجرائم الإلكترونيّة وفقا لقانون العقوبات الجزائريّ: لقد أورد قانون العقوبات الجزائريّ في القسم السّابع مكرّر من الفصل الثّالث الذي يتحدّث فيه المشرّع عن الجنايات والجنح ضدّ الأموال، تحت عنوان: المساس بأنظمة المعالجة الآليّة للمعطيات في القانون رقم 04-05 المؤرّخ في 10 نوفمبر 2004، حيث ينصّ على ما يلي[12]:

- "**المادّة 394 مكرّر:** "يُعاقب بالحبس من ثلاثة أشهر إلى سنة، وبغرامة من خمسين ألف إلى مئة ألف دينار، كلّ من يدخل أو يبقى عن طريق الغشّ في كلّ أو جزء من المنظومة للمعالجة الآليّة للمعطيات، أو يحاول ذلك.

تضاعف العقوبة إذا ترتّب عن ذلك حذف أو تغيير لمعطيات المنظّمة.

وإذا ترتّب عن الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة، تكون العقوبة الحبس من 06 أشهر إلى سنتين، وغرامة من خمسين ألف إلى مئة وخمسين ألف دينار.

- **المادّة 384 مكرّر 1:** "يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 500.000 دج إلى 2000.000 دج كلّ من أدخل بطريقة الغشّ معطيات في نظام أو أزال أو عدّل بطريقة الغشّ المعطيات التي يتضمّنها".

• **المادة 394 مكرّر 2:** "يعاقب بالحبس من شهرين إلى 03 سنوات، وبغرامة من 1000.000 دج إلى 5000.000 دج كلّ من يقوم عمدا وعن طريق الغشّ بما يلي:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتّجار في معطيات مخزّنة أو معالجة أو مراسلة عن طريق منظومة معلوماتيّة يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال لأيّ غرض كان المعطيات المتحصّل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

• **المادّة 394 مكرّر 3:** "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدّفاع الوطنيّ، أو الهيئات والمؤسّسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشدّ".

• **المادّة 394 مكرّر 4:** "يعاقب الشّخص المعنويّ الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرّات الحدّ الأقصى المقرّر للشّخص الطّبيعيّ".

• **المادّة 394 مكرّر 5:** "كلّ من شارك في مجموعة أو في اتّفاق تألّف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التّحضير مجسّدا، أو عدّة أفعال مادّيّة يعاقب بالعقوبات المقرّرة للجريمة ذاتها".

• **المادّة 394 مكرّر 6:** "مع الاحتفاظ بحقوق الغير حسن النّيّة، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع التي تكون محلاّ لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على إغلاق المحلّ أو مكان الاستغلال، إذا كانت الجريمة قد ارتكبت بعلم مالكها".

• **المادّة 394 مكرّر 7:** "يعاقب على الشّروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقرّرة على الجنحة ذاتها". إنّ هذه المواد تحدّد الجريمة والعقاب المقرّر لها من طرف المشرّع الجزائريّ، وهذه العقوبات معمول

بها من طرف القضاة في الواقع إذا ثبتت التّهمة في حقّ المتّهم، ولكنّ الصّعوبة تكمن في كيفيّة إثبات الجريمة وفاعلها.

7- أسباب الجريمة الإلكترونيّة على المستوى الفرديّ والمجتمعيّ والكونيّ: يمكن حصر بعض هذه الأسباب في نظر الدكتور (ذياب موسى) في مستويات ثلاث كما يلي:

أ/ على المستوى الفرديّ: إنّ من بين أسباب الجريمة على المستوى الفرديّ ما يلي ذكره:

- **البحث عن التّقدير:** هناك بعض الجرائم الإلكترونيّة التي يرتكبها شباب طائش وصغار السّنّ من باب التّحدّي وحبّ الظّهور في الإعلام؛

- **الفرصة:** لقد وفّرت التّقنيّات الحديثة والإنترنيت فرصا غير مسبقة لانتشار الجريمة الإلكترونيّة، وإنّ الفرصة لتنتج الجريمة، كما تلعب البيئة وترتيباتها دورا كبيرا في ذلك، والخروج عن القواعد الاجتماعيّة، فوقت الانحراف عن قواعد الامتثال ليلا ونهارا وفي أيّ مكان وعدم وجود رقابة، كلّها عوامل تزيد من فرصة ارتكاب الجريمة الإلكترونيّة، وقد تشكّل المعلومات هدفا سهل المنال لتحقيق المنفعة السّريعة بسرقتها، فهي فرصة مربحة قليلة المخاطر، واحتماليّة الكشف للفاعل فيها ضئيلة"[13]؛ ويدلّ ذلك على أنّ للجاني دوافع في نفسه يريد تحقيقها لفرض وجوده وإثبات نفسه والاعتراف بقيمته داخل المجتمع، ربّما لإحساسه بالنّقص ولامبالاة المحيطين أو الغير به، وبالتالي يكون الإنترنيت هو الذي يتيح له الفرصة المناسبة لتحقيق ذاته من خلال الجريمة الإلكترونيّة التي يرتكبها عن قصد أو عن غير قصد.

- **ضبط الذّات المنخفض:** "تنطلق هذه الدّراسة من النّظريّة العامّة في السّلوك الطّائش، وتؤكّد هذه النّظريّة أنّ احتمال انخراط الأفراد في فعل إجراميّ، يحدث بسبب وجود الفرصة، مع توفّر سمة شخصيّة من سمات الضّبط المنخفض. والسّلوك الطّائش هو كلّ فعل يقوم على القوّة والخداع لتحقيق الرّغبات الذّاتيّة ولهذا يعدّ مظهرا من مظاهر الضّبط الذّاتيّ المنخفض، ذلك أنّ كلّ فرد قد يندفع

لتحقيق مصالحه الشّخصيّة، بما في ذلك السّلوك الطّائش"[14]؛ وهنا تلعب المدرسة والجمعيّات الثّقافيّة دورا بارزا في الحدّ من الجريمة بصفة عامّة والجريمة الإلكترونيّة بصفة خاصّة، وذلك عن طريق حملات التّوعية والتّحسيس بمخاطر الاستخدام الطّائش للإنترنيت، وبخاصّة من طرف الأطفال.

– **الضّغوط العامّة:** "تُرجع نظريّة الضّغوط العامّة الانحراف وخرق القانون إلى دافع ناجم عن قوى البناء الاجتماعيّ، أو استجابات النّفس الاجتماعيّة للحوادث والظّروف التي تكوّن ضغوطات أو مقلقات خاصّة عندما لا تتاح للأفراد الفرصة لتحقيق أهدافهم المقبولة اجتماعيّا"[15]؛ ومعنى ذلك أنّ المشاكل الأسريّة والاجتماعيّة كالفقر والبطالة والآفات الاجتماعية كالمخدّرات والصّحبة السّيّئة، من شأنها أن تجعل الفرد يميل إلى الإجرام الإلكترونيّ، والفراغ أو عدم العمل والانشغال بالدّراسة أو العلم عوامل تسبّب الانشغال بالإنترنيت وتوظيفه في ما يضرّ بصاحبه والغير.

– **النّشاط الرّوتينيّ:** إنّ الرّوتين عبارة عن تكرار العمل نفسه في اليوم أو كلّ الأيّام، على الأقلّ لمدّة زمنيّة طويلة، حتّى يملّ الشّخص فيصاب بالإحباط والتّعب في البدن والعقل، فيميل إلى أشياء أخرى من بينها الإنترنيت؛ إذ "يرى (كوهين وفيلسون) أنّه من المرجّح أن تحدث الجريمة عندما تتلاقى ثلاثة عوامل هي: الجاني المتحفّز، والهدف المناسب، وغياب الحراسة."[16]؛ أي أنّ الجريمة بصفة عامّة والإلكترونيّة بصفة خاصّة تتحقّق بتوفّر الشّروط التي ذُكرت سالفا، وهي الرّغبة الملحّة لدى الجاني ووجود الضّحيّة الفريسة وعدم وجود رقيب، وهذا الشّرط الأخير دائم التّحقّق وكذا الشّرطان الأوّلان في ما يخصّ الجريمة الإلكترونيّة.

ب/ أسباب الجريمة على المستوى المجتمعيّ: إنّ من أسباب ارتكاب الجريمة على مستوى المجتمع ما يلي:

– **التّحضّر:** "يرى (ميك) أنّ التّحضّر سبب رئيس للجرائم الإلكترونيّة في نيجيريا، وأنّ التّحضّر دون الجريمة مستحيل... ممّا يجعلهم يلتفّون إلى الاستثمار

في الجريمة الإلكترونيّة؛ حيث لا تتطلّب رأس مال كبير والتي تعرف أولا الياهو "Yahoo"[17]؛ ومعنى ذلك أنّ الحضارة والتّقدّم من أسباب وجود هذه الجرائم التي ترتكب في الإنترنيت وبواسطة الحاسوب؛

– **البطالة:** إنّ البطالة التي تعني عدم توفّر مناصب الشّغل التي تكفي الشّخص نفسه، وتجعله منشغلا بذاته يتحصّل على رزقه بيده، وتمنعه سؤال الناس، من الأسباب الرّئيسة التي تجعل الإنسان يميل إلى الإجرام بواسطة الإنترنيت تعبيرا عن بعض غضبه من المجتمع؛

– **الضّغوط العامّة:** إنّ الضّغوطات التي تنتاب الفرد كالأمّيّة، والفقر، والجهل والمشاكل والآفات الاجتماعيّة المختلفة من شأنها أن تجعل الفرد يميل إلى شيء آخر هو الانشغال بالإنترنيت؛ وبالتّالي تحقيق نزواته غير المسموح بها اجتماعيّا عن طريق الحاسوب، ومنها إلحاق الضّرر بالغير ويعني ذلك ارتكاب الجريمة الإلكترونيّة؛

– **البحث عن الثّراء:** إنّ الإنترنيت ومعرفة تقنيّات الحاسوب المختلفة من شأنها أن تجعل صاحب هذه المعرفة الخاصّة أن تجعله ثريّا، وذلك عن طريق الجرائم التي يرتكبها بواسطة الإنترنيت، كسرقة الأموال العامّة مثلا، أو التجسّس السّياسيّ، وغالبا ما يقوم بهذا النّوع من الجرائم المتعلّمون والتّقنيّون والخبراء في الحاسوب والإنترنيت؛

– **ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونيّة:** إنّ عدم مواكبة العصرنة والرّقمنة في جهاز العدالة، وعدم توفّر التّقنيّات الحديثة في المحاكم والمجالس القضائيّة، وبالتّالي سريان هذا القطاع بالطّريقة التّقليديّة واستعمال الورق، من شأن كلّ ذلك أن تكثر الجرائم وإفشاء السّرّ المهنيّ المتعلّق بالمهنة وإخراج الملفّات، وغير ذلك.

ج/ أسباب الجريمة على المستوى الكونيّ: إنّ من بين أسباب الجريمة الإلكترونيّة على المستوى الكونيّ ما يلي:

- **التّحوّل للمجتمع الرّقميّ:** من أهمّ سمات عصر المعلومات السّمات الثّلاث الرّئيسة التّالية:

أ/ "**تغيّرات كمّيّة:** في مقدار المعلومات المتدفّقة ونوعيّتها، فبفعل تكنولوجيا الاتّصالات والمواصلات، فإنّ الصّور والمعلومات تغطّي كافّة المعمورة بسرعة ودقّة.

ب/ إرسال المعلومات إلى العديد من الأطراف: البشر والمعدّات، فالمعلومات توجّه الصّاروخ والصّحفيّ يرسل التّقرير والبثّ المباشر من مكان الحدث.

ج/ وجود الشّبكات Networking؛ حيث يتمّ تداول المعلومات بين جميع الأطراف، فتكوّنت التّفاعلات الافتراضيّة، وحلّت محلّ التّفاعل وجها لوجه، وتكوّن المجتمع الافتراضيّ"[18]؛ ومعنى ذلك أنّ الشّبكة العنكبوتيّة قد ربطت أطراف العالم بعضها بعضا، وجعلته قرية صغيرة، وقد اقتصرت المسافة، حيث يمكن رؤية الشّخص والحديث معه من الجزائر وهو في أمريكا مثلا؛

- **العولمة:** "هذا العصر يتطلّب مؤسّسات أمنيّة مصمّمة للتّعامل مع التّغيّر السّريع، تركّز على الإبداع والشّفافيّة وإرضاء العملاء –المجتمع بأسره– مؤسّسات ذات سرعة عالية في نشر المعلومات وقادرة على إعادة تصميم ذاتها لمواجهة المستجدّات السّريعة التّغيّر في عالم الجريمة الإلكترونيّة.

- **التّرابط الكونيّ:** هناك عامل يمكن أن يسهم في دفع مستويات الجريمة يتمثّل في ظهور التّرابط العالميّ في سياق تحوّلات العالم الاقتصاديّة والدّيموغرافيّة بحلول عام 2050، وإنّ العالم سوف يشهد تضاعف عدد سكّان الحضر إلى 6,5 مليار، أي 70 في المئة من سكّان العالم المتوقّع من 8,9 مليار"[19]؛ ومعنى ذلك أنّ ظاهرة العصر المتمثّلة في العولمة التي تعني التّقدّم الباهر والمذهل في كافّة المستويات، فقد عرفنا اليوم ما يسمّى بمجتمع المعرفة والحكومة الذّكيّة، والتّقدّم التّكنولوجيّ وتطوّر الأقمار الصّناعيّة أسهمت كلّها في الميل أكثر إلى ارتكاب الجرائم الإلكترونيّة المختلفة.

• **انكشاف البنية التّحتيّة المعلوماتيّة الكونيّة:** "تتفاوت البنى التّحتيّة المعلوماتيّة بدرجة انكشافها إلى الكوارث الطّبيعيّة والإهمال البشريّ وسوء التّصرّف الإنسانيّ، وقد حدّد التّقرير الرّئاسي الأمريكيّ بخصوص حماية البنية التّحتيّة الحسّاسة خمسة (05) قطاعات بناءً على الخصائص المشتركة لها ومن بينها قطاع الاتّصالات والمعلومات؛ وتشمل شبكات الاتّصالات العامّة PTN والإنترنيت، والحاسبات في المنازل، والاستخدام الأكاديميّ والحكوميّ والتّجاريّ"[20]؛ ويدلّ ذلك على أنّ التّطوّر التّقنيّ وتزايد عدد وتطوّر كيفيّة مستخدمي الإنترنيت سبب في تزايد وقوع الجريمة الإلكترونيّة.

د/ أسباب تتعلّق بخصائص الجريمة الإلكترونيّة[21]: في ما يلي مجموعة من خصائص الجريمة الإلكترونيّة، والتي تؤدّي إلى ارتكاب الجريمة الإلكترونيّة ومنها:

- **الإزالة:** الجريمة لا تتطلّب الإزالة فيمكن نسخها فقط؛
- **التّوافر:** المعلومات في كلّ مكان جاهز لتستهدف الجريمة الإلكترونيّة؛
- **القيمة:** معلومات بطاقات الائتمان والحسابات المصرفيّة والتّصاميم ذات قيمة؛
- **المتعة:** كثير من الجرائم الإلكترونيّة ممتعة مثل سرقة الموسيقى والمال؛
- **الدّيمومة:** المعدّات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة؛
- **سرعة التّنفيذ:** لا يتطلّب تنفيذ الجريمة الوقت الكثير، ففي وقت قصير يمكن أن تنتقل ملايين الدّولارات من مكان إلى مكان، وهذا لا يعني عدم استخدام برامج أو معدّات؛
- **التّنفيذ عن بعد:** يمكن للفاعل تنفيذ جريمته وهو في دولة أخرى، سواء كان ذلك من خلال الدّخول إلى الشّبكة المعنيّة، أو اعتراض عمليّة تحويل ماليّة، أو سرقة معلومات هامّة، أو تخريب؛
- **إخفاء الجريمة:** إذ يمكن للجاني ارتكاب الجريمة وإخفاء بسهولة دون أن يعلم بها أحد لمدّة طويلة من الزّمن؛

- **الجاذبيّة:** غدت أكثر جذبا لاستثمار الأموال وغسيلها وتوظيفها في تطوير تقنيّات وأساليب الدّخول إلى الشّبكات وبيع المعلومات، أو سرقة البنوك، أو استخدام أرقام البطاقات؛

- **عابرة للحدود الدّوليّة:** الأقمار الصّناعيّة؛

- **صعوبة إثباتها:** هذا راجع إلى افتقاد وجود الآثار التّقليديّة للجريمة، وغياب الدّليل الفيزيقي (بصمات، شواهد، تخريب...) وسهولة محو الدّليل، ونقص خبرة الشّرطة، والنّظام العدليّ، وعدم كفاية القوانين القائمة. هذه هي إذًا الخصائص العامّة التي تسهّل ارتكاب الجريمة الإلكترونيّة، فإذا نظرنا إلى السّرعة فالإنترنيت في ثوانٍ معدودات والتّنفيذ عن بعد، وعدم وجود رقيب في السّرقة الخفيّة لرؤوس الأموال، والتّجسّس الإلكترونيّ عن طريق الأقمار الصّناعيّة، ووجود المعلومات في كلّ مكان في الإنترنيت، من شأن كلّ ذلك أن يحفّز الجاني على اقتراف الذّنب وأن يخرج من الجريمة سالما غير مدان.

8- **كيفيّة الحدّ من الجريمة الإلكترونيّة:** هناك بعض الحلول التّقنيّة والبسيطة التي يمكن لأيّ شخص اتّخاذها وسيلة لحمايته من الوقوع في الخطر، وهي سهلة التّطبيق لا تتطلّب جهدا أو مالا، ومنها ما يلي:

- "على مشغّلي الإنترنيت تجنّب الكشف عن أيّ معلومات تتعلّق بهم، مثل بطاقات الهويّة على الموقع؛

- عدم إرسال الصّور عبر الإنترنيت أثناء التّحدّث مع الغرباء؛

- حفظ نسخة احتياطيّة من الملفّات والمجلّدات، بحيث لو فقدت بيانات أو معلومات نتيجة ابتلائها بالفيروسات؛

- عدم استخدام بطاقة الائتمان الخاصّة في حالة عدم التّأكّد من أنّ الموقع آمن، فهذا الإجراء قد يحمي من التّحايل؛

- التّحقّق من المواقع التي يقوم الأطفال بفتحها من أجل تجنّب الإساءة؛

- استخدام برامج حماية أمن الإنترنيت، والتي تمكّن من السّيطرة على ملفّات تعريف الارتباط cookies، لمنع إرسال المعلومات إلى المواقع؛

- استخدام جدران الحماية إلى أقصى حدّ ممكن؛
- الخادمات servers التي تدير مواقع عامّة يجب أن تكون محميّة بشكل منفصل عن شبكة العمليّات؛
- عدم الاحتفاظ بالبيانات الحسّاسة في الحاسب الآليّ مثل البيانات الماليّة والشّخصيّة خشية وقوعها في أيدي السارقين؛
- التّقليل من أخطار الفيروسات أو البرامج الضّارّة بإيقاف البلوتوث والويفي wi-fi، والأشعّة تحت الحمراء، وعدم تشغيلها إلاّ عند الحاجة؛
- إغلاق البلوتوث في الأماكن العامّة، وعدم قبول طلب اتّصال إلاّ من أشخاص موثوق بهم؛
- عدم استخدام وتثبيت البرامج المجّانيّة غير الموثوق بها؛ لأنّ عددا كبيرا منها يقوم بتثبيت برامج تجسّس ودعاية"[22]؛ ومعنى ذلك أنّ بإمكان مستخدم الحاسب الآليّ وبالتّالي الإنترنيت أن يقوم بحماية نفسه عن طريق عدم نشر صوره في الإنترنيت، وصيانة جهازه من الفيروسات، وعدم الإفصاح عن هويّته الحقيقيّة، بل الاكتفاء بالأسماء والصّور المستعارة، وعدم حفظ البيانات القيّمة فيه، وهذه كلّها مجرّد وقاية من الخطر ليس إلاّ.

- **ومن سبل الوقاية القانونيّة من الجريمة الإلكترونيّة هذه التي سأوردها في ما يلي:**

1/ التّفتيش: هو إجراء من إجراءات التّحقيق يقوم به موظّف قانونيّ مختصّ في مكان قانونيّ قضائيّ خاصّ، بهدف الوصول إلى المعلومات التي تساعد على إيجاد الحلّ أو فكّ لغز الجريمة، ولكن هل يمكن تطبيق هذا التّفتيش الكلاسيكيّ لاكتشاف معالم الجريمة الإلكترونيّة؟

أوّلا: المكوّنات الماديّة للحاسب الآليّ: "لا يختلف اثنان في أنّ الولوج إلى المكوّنات الماديّة للحاسب الآليّ بحثا عن شيء ما يتّصل بجريمة إلكترونيّة، يفيد في كشف الحقيقة عنها وعن مرتكبها، يخضع للإجراءات القانونيّة الخاصّة بالتّفتيش؛ بمعنى أنّ من الأماكن العامّة أو الخاصّة، ولصفة المكان وطبيعته أهميّة

قصوى، فإذا كانت الجريمة موجودة في مكان خاص كمسكن المتّهم أو أحد ملحقاته، كان لها حكمه، فلا يجوز التّفتيش إلا في الحالات التي يجوز فيها تفتيش مسكنه[23]؛ حيث لا يجوز تفتيش الأماكن العامّة إلاّ طبقا للقواعد التي يقرّرها القانون.

ثانيا: المكوّنات المنطقيّة للحاسب الآليّ: يتضمّن التّفتيش أيضا البيانات المتعلّقة بالحاسب الآليّ الموجودة داخليّا، بالرّغم من الاختلاف الفقهيّ في هذا الصّدد، حول ما إذا كان المفهوم المادّيّ ينطبق على المفهوم المعنويّ، مع العلم بوجود قصور ونقص تشريعيّ في ذلك.

ثالثا: شبكات الحاسب الآليّ: "يمكن أن تمتدّ شبكات الحواسب عالميّا وليس فقط محلّيّا، وهنا أُثِيرَت مشاكل قانونيّة عويصة حول إمكانيّة التّفتيش أم لا، ولذلك ظهرت آراء فقهيّة دوليّة كثيرة، وبالتالي هناك من الدّول من رأت ضرورة إصدار اتّفاقيّات دوليّة خاصّة بالتّفتيش في مثل هذه الحالة"[24]، وبالتّالي لابدّ من الاتّحاد والتّعاون الدّوليّ المشترك للحدّ من الجريمة الإلكترونيّة؛ إذ سمحت أغلب الدّول بالإنصات للوصول إلى المعلومات الحقيقيّة التي من شأنها أن توقف أو تحدّ من ارتكاب الجرائم عبر الإنترنيت أو بواسطته.

وحول هذه النّقطة بالذّات، فقد أخذ المشرّع الجزائريّ بهذا المبدأ في قانون الإجراءات الجزائيّة الجزائريّ، حيث نصّت المادّة 65 مكرّر 05 على ما يلي:

"إذا اقتضت ضرورات التّحرّي في الجريمة المتلبّس بها، أو التّحقيق الابتدائيّ في جرائم المخدّرات، أو الجريمة المنظّمة العابرة للحدود الوطنيّة، أو **الجرائم الماسّة بأنظمة المعالجة الآليّة للمعطيات،** أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلّقة بالتّشريع الخاصّ بالصّرف، وكذا جرائم الفساد، يجوز لوكيل الجمهوريّة المختصّ أن يأذن بما يلي:

- اعتراض المراسلات التي تتمّ عن طريق وسائل الاتّصال السّلكيّة واللاّسلكيّة؛

– وضع التّرتيبات التّقنيّة، دون موافقة المعنيّين، من أجل التقاط وتثبيت وبثّ وتسجيل الكلام المتفوّه به بصفة خاصّة أو سرّيّة من طرف شخص أو عدّة أشخاص يتواجدون في مكان خاص"[25]؛ ومن فحوى هذه المادّة القانونيّة، نستنتج أنّ التّشريع الجزائريّ قد أورد الموادّ القانونيّة التي تجرّم أمثال هذه الجرائم، وللقاضي السّلطة التّقديريّة في قياس وتقدير حجم الضّرر لإصدار الحكم على الجاني.

2/ المعاينة: "لغةً بمعنى النّظر، وعاين الشّيء رآه بعينه، ودلالتها القانونيّة وبخاصّة في المجال الجنائيّ هي التي تعتمد حاسّة البصر، وتبعا لذلك تعني المعاينة رؤية أماكن ارتكاب الوقائع الجنائيّة، كما تنصرف إلى فحص جسم المجنيّ عليه والمتّهم، وإثبات ما يوجد بها من آثار، كما عرّفها جانب من الفقه بأنّها مشاهدة وإثبات الحالة في مكان الجريمة"[26]؛ إذ تكمن أهمّيّة المعاينة في تصوّر كيفيّة وقوع الجريمة، وظروف وملابسات القضيّة للتّأكّد منها، وجمع المعلومات وضبطها والتّحقيق فيها.

إنّ مسرح الجريمة المادّيّة المرتكبة بالطّريقة التّقليديّة كالقتل أو السّرقة مثلا يمكنه أن يتغيّر، بحيث يسهل محو البيان أو الأدلة والبصمات عن طريق المسح وغير ذلك، والشّيء نفسه ينطبق على الجريمة الإلكترونيّة؛ حيث "إنّ مسرح الجريمة الإلكترونيّة يتمثّل في الموقع أو المكتب الذي توجد فيه المعدّات والأنظمة المعلوماتيّة التي كانت محلاّ للجريمة، أو أداتها"[27]؛ لأنّ الجهاز يحتوي على سطح المكتب والبيانات المختلف المتواجدة داخله، والتي فيها يتمّ البحث عن الأدلّة.

غير أنّ مسرح الجريمة في الإنترنيت محلّ تردّد عدّة أشخاص عليه في الثّانية الواحدة، ومن أجل تفادي أيّ خلل في المعاينة، **يجب تتبّع الإرشادات الفنّيّة التّالية:**

– "تصوير الحاسب والأجهزة الطّرفيّة المتّصلة به، على أن يتمّ تسجيل وقت وتاريخ ومكان التقاط كلّ صورة؛

– العناية بملاحظة الطّريقة التي يتمّ بها إعداد النّظام؛

– ملاحظة وإثبات حالة التّوصيلات والكابلات المتّصلة بكلّ مكوّنات النّظام حتّى يمكن إجراء عمليّات المقارنة والتّحليل حين عرض الأمر على المحكمة؛

– عدم نقل أيّ مادّة معلوماتيّة من مسرح الجريمة قبل إجراء اختبارات، للتّأكد من خلوّ المحيط الخارجيّ لموقع الحاسب من أيّ مجال لقوى مغناطيسيّة، يمكن أن تتسبّب في محو البيانات المسجّلة؛

– التّحفّظ على معلومات سلّة المهملات من الأوراق الملقاة أو الممزّقة وأوراق الكربون المستعملة والشّرائط والأقراص المغناطيسيّة غير السّليمة وفحصها، وترفع عليها البصمات ذات الصّلة بالجريمة؛

– قصر ومباشرة المعاينة على الباحثين والمحقّقين الذين تتوفّر لهم الكفاءة العلميّة، والخبرة الفنّيّة في مجال الحاسبات"[28]؛ والجدير بالملاحظة هو أنّ تطبيق هذه الإرشادات التي يقدر عليها سوى التّقنيّون والخبراء في الإعلام الآليّ والشّرطة العلميّة القضائيّة.

ويتمّ توثيق مسرح الجريمة الإلكترونيّة من خلال الأدلّة الموجودة على **الورق** وعلى **جهاز الحاسب الآليّ وملحقاته**؛ "حيث إنّ وجود جهاز الحاسب الآليّ مهمّ جدّا للقول بأنّ الجريمة الواقعة، هي جريمة معلوماتيّة أو جريمة حاسوبيّة، وإنّها مرتبطة بالمكان أو الشّخص الحائز على الجهاز. ولأجهزة الحاسب الآليّ أشكال وأحكام وألوان مختلفة، ويجب توفّر خبير بالحاسب الآليّ من أجل القيام بالإجراءات التّقنيّة الضّروريّة. ويتمّ التّوثيق أيضا على **البرمجيّات**؛ إذا كان الدّليل الرّقميّ ينشأ باستخدام برنامج خاص، أو ليس واسع الانتشار، فإنّ أخذ الأقراص الخاصّة بتثبيت وتنصيب هذا البرنامج أمر مهمّ عند فحص الدّليل. كما يتمّ التّوثيق على وسائط التّخزين المتحرّكة؛ كالأقراص المدمجة –أقراص اللّيزر– والأقراص المرنة والأشرطة المغناطيسيّة. وتعدّ هذه الوسائط جزءً من الجريمة المرتكبة عبر الإنترنيت متى كانت محتوياتها عنصرا من عناصر الجريمة. ويتمّ التّوثيق أيضا على **المراشد** الخاصّة بالمكوّنات المادّيّة والمنطقيّة للحاسب الآليّ، والتي تفيد في معرفة التّفاصيل الدّقيقة لكيفيّة عملها. ويتمّ التّوثيق أيضا على **المودم**؛ إذ هو الوسيلة التي تمكّن أجهزة الحاسب الآليّ من الاتّصال بعضها ببعض عبر خطوط الهاتف، وفي الوقت الحاليّ تطوّر المودم ليكون جهاز إرسال واستقبال الفاكس

والرّدّ على المكالمات الهاتفيّة، وتبادل البيانات وتعديلها"[29]؛ ويعني ذلك أنّ العلم في هذا الميدان يتطلّب الخبرة الطّويلة والسّرعة في التّنفيذ أيضا؛ لأنّ إدراك الدّليل لا يحتمل التّأخير، وإلاّ غاب الجاني عن الأنظار وبقي الضّرر يحفر عميقا في نفس الضّحية.

3/ الخبرة: إنّ الخبرة تعني اكتساب الخبير الشّطارة والمعرفة التّقنيّة والطّويلة نتيجة المدّة الزّمنيّة المديدة التي أمضى فيها تجربته المهنيّة، والتي بمقتضاها أصبح صاحب تجربة مهنيّة وخبرة كبيرة في تخصّصه العمليّ، وتتمّ الاستعانة بخبير في الحالات التّالية:

- "تزوير المستندات المدخلة في أنظمة الحاسبات الآليّة أو النّاتجة بعد المعالجة؛
- التّلاعب في البيانات؛
- التّلاعب في البرامج الأساس أو برامج التّطبيقات؛
- الغشّ أثناء نقل وبثّ البيانات"[30]؛ وذلك إن دلّ على شيء إنّما يدلّ على أنّ الخبرة ضروريّة الحضور في هذا النّوع الخاصّ من الجرائم الإلكترونيّة، وبخاصّة المتعلّقة بالتّزوير الذي يعرف اليوم أوجّ التّقنيّات؛ بحيث يصعب على المحقّقين القضائيّين وعلى الشّرطة الوصول إلى الحقيقة.

- **خاتمة:** إنّ أحسن ما نختم به هذا البحث البسيط المندرج ضمن ملتقى راقٍ مندرج ضمن أمن المعلومات، هو تقديم بعض النّصائح للآباء وربّات البيوت مفادها مراقبة الأطفال مراقبة دائبة –وذلك من الصّغر– حالما يلحّون على استعمال الكمبيوتر؛ حيث إنّ التّربية السّليمة من شأنها أن تمنع وقوع الحوادث والجرائم الخطيرة بواسطة الإنترنيت، بالإضافة إلى توعية التّلاميذ في المدارس سواء الخاصّة منها أم العامّة بضرورة أخذ الحيطة والحذر عند استعمال الإنترنيت. هذا بغضّ النّظر عن الجمعيّات الثّقافيّة التي تسهم في تقليص حجم الضّرر النّاجم عن الاستخدام العشوائيّ وغير الأخلاقيّ ولا المناسب للجهاز الآليّ.

الإحالات:

1- محمد سعيد جعفور، مدخل إلى العلوم القانونيّة – الوجيز في نظريّة القانون، د ط. دار هومه الجزائر: 1998، ص 13، نقلا عن: حبيب إبراهيم الخليلي، المدخل للعلوم القانونيّة –النّظريّة العامّة للقانون، ط 2. د ب: 1998، ص 9.

2- رابحي أحسن "الجريمة الإلكترونيّة: النّقطة المظلمة بالنّسبة للتّكنولوجيّة المعلوماتيّة" جامعة محمّد بوقرة، بومرداس، المجلّة الجزائريّة للعلوم القانونيّة الاقتصاديّة والسّياسيّة، جامعة الجزائر عدد 01، الجزائر: 2011، ص 226.

3- ذياب موسى البداينة "الجرائم الإلكترونيّة: المفهوم والأسباب" عدد خاص بالملتقى العلميّ حول: الجرائم المستحدثة في ظلّ المتغيّرات والتّحوّلات الإقليميّة والدّوليّة خلال الفترة من 2-4 سبتمبر 2014، كلّيّة العلوم الاستراتيجيّة، الأردن: 2014، ص 3.

3- المرجع نفسه، ص 5.

4- رابحي أحسن، "الجريمة الإلكترونيّة: النّقطة المظلمة بالنّسبة للتّكنولوجيّة المعلوماتيّة" ص 224.

5- المرجع نفسه، ص 225.

6- ذياب موسى البداينة "الجرائم الإلكترونيّة: المفهوم والأسباب" ص 7.

7- رابحي أحسن "الجريمة الإلكترونيّة: النّقطة المظلمة بالنّسبة للتّكنولوجيّة المعلوماتيّة" ص 229.

8- المرجع نفسه، ص 231.

9- المرجع نفسه، ص 231.

10- فايزة قاسم، الجريمة المعلوماتيّة في ظلّ قانون العقوبات الجزائريّ، مذكّرة لنيل شهادة الماجستير في القانون، كلّيّة الحقوق، جامعة تيارت: 2011، ص 145، 146.

11- المرجع نفسه، ص 134.

12- ذياب موسى البداينة "الجرائم الإلكترونيّة: المفهوم والأسباب" ص 10.

13- المرجع نفسه، ص 11.

14- المرجع نفسه، ص 12.

15- المرجع نفسه، ص13.

16- المرجع نفسه، ص 14

17- المرجع نفسه، ص15.

18- المرجع نفسه، ص 17 .

19- المرجع نفسه، ص 18.

20- المرجع نفسه، ص 19 – 20.

21- وزارة الدّاخليّة، المديريّة العامّة للاتّصالات والمعلوماتيّة، د ط. مديريّة تكنولوجيا المعلومات، قسم نظم المعلومات، شعبة أمنيّة المعلومات، د ب: د ت، ص 13.

22- يوسف صغير، الجريمة المرتكبة عبر الإنترنيت، مذكّرة لنيل شهادة الماجستير في القانون الأساسي والعلوم السّياسيّة، جامعة مولود معمّري، تيزي-وزّو، كلّيّة الحقوق: 2013، ص 77 نقلا عن: حسين بن سعيد الغافريّ "التّحقيق وجمع الأدلّة في الجرائـــم المتعلّقة بشبكة الإنترنيت" ص 11، مقال متوفّر على الموقع: http://www.eastlaws.com،

23- المرجع نفسه، ص 80.

24- المادّة 65 مكرّر 05 من القانون رقم 06-22 المؤرّخ في 22 ديسمبر 2006، المعدّل والمتمّم لقانون الإجراءات الجزائيّة، جريدة رسميّة عدد 84.

25- يوسف صغير، المرجع السابق، ص 82.

26- المرجع نفسه، ص 85، نقلا عن: عبد الفتّاح بيومي حجازي، مبادئ الإجراءات الجنائيّة في جرائم الكمبيوتر والإنترنيت -دراسة متعمّقة في جرائم الحاسب الآليّ والإنترنيت، بهجات للطّباعة والتّجليد، مصر: 2009.

27- المرجع نفسه، ص 86، نقلا عن: محمّد أبو العلا عقيدة، ص 7-8.

28- المرجع نفسه، ص 87، نقلا عن: حسين بن سعيد الغافريّ، التّحقيق وجمع الأدلّة في الجرائم المتعلّقة بشبكة الإنترنيت، ص 10-11.

29- المرجع نفسه، ص 90.

Internet et vie privée

Aldjia OUTALEB
Maitre de conférences HDR
Université de Tizi Ouzou

Résumé : Le web est l'« aspirateur » de tout ce qu'il trouve sur son chemin. Toutes les données y compris les comportements que chaque internaute fournit partent, sans nécessairement le vouloir, dans de gigantesques bases.

Mais, qu'est-ce que les données personnelles ?

C'est en fait, tout ce qui permet d'identifier une personne : son nom, son prénom, sa date de naissance, l'adresse de son domicile, son numéro de téléphone...

Ces informations sont souvent demandées pour rejoindre un forum de discussions, pour mettre des photos en ligne, pour poster un commentaire...

Il est tout à fait clair que ces données servent à produire de nouvelles applications qui vont faciliter la vie de l'internaute. En revanche,

- À quoi d'autre encore ces données sont-elles utilisées ?
- Y a-t-il un danger ?
- Quelle est l'ampleur de ce danger ?

Pour développer le thème d' « Internet et vie privée », nous irons à la rencontre des personnes pour recueillir, à l'aide d'un questionnaire-débat, leurs représentations sur l'utilisation des nouvelles technologies, en l'occurrence Internet, et la protection de leur vie privée.

Pour tenter de répondre à ces questions, il convient d'abord de considérer les nouveaux outils de communication, leur convergence et leur intégration ; puis d'analyser les conséquences de ces nouvelles formes d'échanges électroniques et leur impact sur les relations entre et avec les usagers.

Mots clés : Internet – vie privée – algériens

Introduction

Internet a envahi notre vie quotidienne, de ce fait, elle a considérable changé. Internet est à la fois un moyen de communication par lequel nous pouvons échanger et exprimer nos opinions ; un media commercial qui permet de vendre. C'est également un outil de recherche qui permet d'accéder au savoir ; un outil de paiement, un outil de jeux ; un GPS ; une télévision…

Parallèlement, aujourd'hui, nous ne pouvons plus passer inaperçu. Nous sommes en effet surveillés et fichés dans de nombreuses occasions. Dans la plupart des situations, les individus sont invités à fournir eux-mêmes des renseignements les concernant, aussi bien dans le cadre de leurs relations personnelles que professionnelles (par exemples, lors d'un entretien d'embauche, inscription à un concours…), ou encore lors de démarches administratives. Depuis les années 1990, les technologies de l'information et de la communication ont rendu cette collecte plus efficace et plus rentable.

Aussi, l'intrusion de la technologie dans nos vies privées s'applique-t-elle à tous les domaines : santé, transports, loisirs... Prenons des exemples simples : la carte de crédit qui permet de retracer les déplacements et les achats détaillés d'une personne, la vidéosurveillance qui permet d'identifier et donc de retrouver un individu dans une foule...

Nous nous demandons :

- Quel est donc cet univers où tout le monde sait ce que l'on fait ?
- Où et quand s'arrête la surveillance des personnes ?
- Où et quand commence la vie privée ?

Dans un tel cas, il est impératif de reprendre en main nos données personnelles sans pour autant s'éloigner des précieux services de l'Internet ! Et notamment, ne pas accepter toutes les conditions d'utilisations proposées par les différents sites et réseaux sociaux.

Constitution du corpus : Pour mener à bien notre étude sur l' « Internet et vie privée », nous avons mené un questionnaire-débat avec diverses personnes. Nos interlocuteurs, de tous les âges appartiennent à différentes catégories sociales : enseignants, étudiants commerçants, citadins, villageois, jeunes…

Le thème de l'Internet et le respect de la vie privée a provoqué beaucoup de réactions et d'interactions chez et avec nos interlocuteurs et a suscité chez certains beaucoup d'émotions et d'étonnements ….

Notre questionnaire est composé de questions telles :

1. Avez-vous une connexion internet chez vous ?
2. Combien d'heures, en moyenne par jour, vous connectez-vous ?
3. A quoi Internet vous sert-il ?
4. Surfez-vous sur des réseaux sociaux ? Lesquels ?
5. Avez-vous un compte ou une boite ou plusieurs ? A quoi servent-ils ?
6. A quoi comparez-vous Internet ? Pourquoi ?
7. Que pensez-vous de la vie privée des internautes ? Pensez-vous à la protéger ? Comment ?
8. Internet transforme-t-il la vie familiale ?
9. Les technologies actuelles permettent de suivre les individus à la trace. Le savez-vous ?
10. Etes-vous inquiets sur la protection de votre vie privée ?
11. Utilisez-vous des pseudonymes ? Qu'en pensez-vous ?
12. Vous a-t-on déjà piraté un de vos comptes ?

Analyse et commentaires du corpus

La présence d'Internet dans la vie quotidienne : Plusieurs études (Patrick Giroux, Mathieu Gagnon : 2011) menées récemment permettent de mieux appréhender l'importance réelle d'Internet dans la vie d'aujourd'hui. La consommation d'Internet augmente régulièrement, au point que ce média est maintenant plus important que la télévision.

Selon les mêmes études, les internautes raffolent des réseaux sociaux. Internet est devenu un lieu où ils se rencontrent, discutent échangent, partagent…

Le nombre d'internautes qui se connectent quotidiennement a fortement progressé durant les deux dernières années.

A la question : « avez-vous internet chez vous ? » les jeunes notamment se sont précipités en même temps pour répondre. Il a fallu les calmer et leur faire respecter une certaine discipline : laisser et surtout accorder la parole aux autres.

Un jeune, impatient, lâche ses premiers propos :

- Avant je n’aimais pas rester à la maison. Maintenant, je n’en sors presque plus. Je suis tout le temps connecté, et par le biais d’Internet et de réseaux sociaux comme Facebook, je peux savoir tout sur tout le monde…eh…eh
- Depuis que nous avons Internet avec Wifi à la maison, je ne regarde plus la télé. Ma tablette me suit partout, même dans mon lit pour ne dire que ça ; lance une jeune fille.
- Avant, j’allais au cyber deux ou trois fois par semaine pour me connecter pendant une heure. J’y mettais tout mon argent de poche. Maintenant qu’on a internet à la maison, le temps ne compte plus et mon argent est dans ma poche !!!

Les jeunes hommes, principalement, sont connectés à longueur de journée. Ils sont adeptes notamment des réseaux sociaux. Ils ne jurent que par Internet !

Les avantages d’Internet : Nous devons souligner les apports positifs du net. C’est pourquoi nous vous demandons de nous en citer quelques uns.

- Effectivement, nous confie un enseignant de français, Internet présente une longue liste d’avantages. Par exemple, nous pouvons faire de la recherche sur des cours, des fiches, des exercices avec les corrections… Nous trouvons une grande quantité et diversité d’informations utiles pour l’enseignement.
- Un commercial d’une agence de voyages nous rappelle que l'internet favorise l'accès à beaucoup de services : réservations administrations électroniques, banques électroniques, bibliothèques numériques, etc.
- Après une longue journée de travail, nous confie un père de famille, on est pressé de rentrer chez soi pour se détendre devant la toile, à regarder des films entiers, des vidéos de son choix sans gêner personne, à écouter la musique que l’on veut. En plus, nous pouvons discuter longuement avec des amis qui se trouvent à l’autre bout du monde.
- lnternet est un excellent moyen de communication, atteste un fonctionnaire. Il nous permet de rester en contact avec nos amis, de leur parler en temps réel, de partager nos goûts, d’évoquer nos souvenirs d’enfance, nos expériences. Internet nous permet également de se faire de nouveaux amis. Grâce à Internet, le monde est à portée de main en un clic.

- Une fille nous rappelle vivement : et moi, j'aime bien la cuisine et c'est grâce à internet que toute la famille se régale : je recherche et trouve des recettes faciles et pas chères à réaliser, je prélève même des vidéos. Internet ? C'est tout simplement génial !

A notre époque chercher l'âme soeur via le net n'est plus un tabou. De nombreuses personnes se connectent sur des sites de rencontres c'est même devenu la meilleure méthode pour trouver le partenaire idéal. Nous avons rencontré trois jeunes hommes qui jusqu'à la découverte d'Internet, étaient célibataires, qui, aujourd'hui, avouent avoir trouvé l'amour sur internet. Ils se confient :

- C'est encore plus facile de connaitre sur internet que réellement. Aujourd'hui hamdoulillah, ça marche très bien entre nous.
- Je l'ai abordée parce que son profil correspondait à mes attentes. Nous étions honnêtes de suite l'un envers l'autre. Nous nous sommes échangé nos comptes Skype. Quelques heures plus tard, nous nous sommes parlé et voilà ! On remercie aujourd'hui internet parce que nous avons plein plein de projets : le mariage en premier.
- J'ai tout de suite donné mes renseignements et mes attentes, je n'ai pas du tout pensé à la protection de ma vie privée. D'ailleurs est-ce que j'avais une vie privée avant ? Non ! Je n'ai rien à cacher et je n'interesse personne sauf maintenant ! Internet m'a beaucoup aidé car je suis très timide de nature…

Les inconvénients d'Internet : De toute évidence, comme nous venons de le voir à travers notre enquête, l'Internet est un outil remarquable qui aide les personnes de tous âges à apprendre, à se cultiver et à communiquer de manières inespérées. Cependant, comme la plupart des outils, il peut devenir une arme s'il est utilisé avec malice et/ou insouciance. Et sans aucun doute, Internet a ses mauvais côtés, ses prédateurs et ses victimes. En effet, ce monde virtuel qu'est internet est le paradis pour ceux qui veulent apprendre, connaitre d'autres cultures, découvrir d'autres pays, d'autres personnes, de nouveaux domaines…

Cependant, si les adultes en sont, généralement, conscients et bien avertis, ce n'est malheureusement pas le cas des jeunes, pour qui Internet peut très vite se montrer dangereux.

- Les premiers dangers qui se présentent sur Internet sont les nombreux virus qui nous font perdre des fichiers importants et font beuguer notre ordinateur, déclare un internaute assidu de la toile.
- Les internautes ne sont pas à l'abri des regards ; des informations personnelles peuvent être divulguées par soi-même ou par un tiers, ce qui peut nuire à la personne, d'autant plus que le net a une grande mémoire et il devient difficile d'effacer ces informations personnelles par la suite, déclare un informaticien comme pour nous avertir.
- J'ai adressé à un ami un email privé dans lequel je racontais mes vacances passées en Tunisie. Par la suite je reçois dans cette même boite des publicités ciblées sur la Tunisie. Etonnant, non ? s'exclame un jeune adolescent.
- La cyberdépendance est également un très gros problème. Je connais des personnes qui restent des heures et des heures devant la toile. Ces gens passent plus de temps sur le net qu'avec leurs amis ou leur famille. Ils croient qu'ils sont chez eux mais en réalité ils sont isolés et en sont totalement absents.
- les hommes sont plus dépendants d'internet que les femmes. Pour les jeux virtuels ou les sites de rencontres notamment, ils deviennent de véritables drogués du web.

A propos de la protection de la vie privée : L'Internet, en l'occurrence les réseaux sociaux, est vu comme un espace privé et qui appartient aux jeunes. C'est un endroit où ils peuvent partager des confidences, se faire des amis, et construire leur personnalité. Les jeunes prennent des risques pour obtenir quelque chose en retour comme l'accès à un jeu, à une application. Ainsi, ils vont innocemment partager des renseignements privés pour des raisons pratiques, ou pour témoigner de leur confiance aux autres.

Ils considèrent les forums comme des places privées, ils discutent donc à bâtons rompus tout en s'en donnant à cœur joie et sans même s'apercevoir qu'ils se trouvent dans un endroit où il se peut qu'il y ait des invasions de la vie privée. Les renseignements partagés peuvent avoir plus d'impacts qu'ils ne l'imaginent.

Une fille dit tout naïvement :

- Moi, j'habite au village, sur Internet, la plupart de mes amis(es) je les connais même réellement puisqu'on se voit presque

tous les jours. Donc, je peux dire que je ne risque rien. Je n'ai aucun intérêt à me soucier, n'est-ce pas ?

- Mais, là soudainement, j'ai peur…l'interrompt un jeune adolescent ; eh, quelles précautions vais-je prendre pour protéger ma vie mais aussi celle des petits frères et soeurs ?

Un autre nous déclare tristement :

- J'ai même entendu parler de crimes, de suicides commis à causes des problèmes générés par des réseaux sociaux.
- Pour certaines personnes, ces réseaux sont parfois utilisés comme outil de vengeance. Un garçon, sous un drôle de pseudonyme a publié des photos de son ex-petite amie qui l'a quitté pour un autre nous confie timidement une jeune fille. Moi, j'ai peur…
- Moi, je m'en fiche, je n'ai absolument rien à cacher, intervient sa voisine…
- La plupart d'entre nous, prétend un jeune averti, ne savent pas au juste à qui nous parlons sur Internet ou qui gère les sites Web que nous consultons. Donc, nous encourons des tas de problèmes si la protection des donnés n'est pas assurée.

La vie privée, c'est la sphère d'intimité de chacun. C'est tout ce qui est personnel et qui ne regarde personne d'autre que soi et ses proches comme sa vie familiale, sentimentale, conjugale, ses croyances, ses opinions…

Tout le monde s'accorde à dire que les utilisateurs d'Internet ont droit au secret sur eux-mêmes. Cependant, la question qui se pose est celle de savoir comment y parvenir.

Le degré de conscience chez les internautes : Les informations que nous communiquons sur notre vie privée peuvent se retourner contre nous.

Les jeunes n'hésitent nullement à parler de leur religion, de leurs goûts, de leur culture. Ils publient leurs coordonnées, leurs photos sans s'en inquiéter aucunement.

- Les dialogues en direct et les messageries instantanées peuvent s'avérer très dangereux et les risques sont alors plus accrus lorsqu'il s'agit d'enfants qui se connectent, nous confie avec inquiétude un père de famille.
- C'est surtout les femmes et les filles qui se montrent réservées. Comme l'exigent les traditions. Mes amies ont toutes des pseudos bizarres sur leurs comptes Facebook. Elles ne publient jamais de

photos dans lesquelles on peut les reconnaitre, affirme une jeune fille comme si elle cherchait à nous rassurer.

- Les vieux se montrent également très discrets, on ne les comprend pas d'ailleurs… Par contre, les jeunes diffusent plus facilement leurs informations personnelles, et exagèrent même sur la description et leurs coordonnées physiques, renchérit son voisin.

Parmi les internautes interrogés, très peu sont décidés à prendre des mesures pour protéger leur identité en ligne :

- Je ne suis pas du tout d'accord avec les méthodes utilisées par Internet, mais je ne vois pas ce que moi je peux y changer, nous apprend fièrement une jeune fille, cadre auprès de la fonction publique.
- Nous sommes conscients qu'il y a et qu'il y aura toujours des fuites sur Internet, déclare un autre internaute, et tout ce que nous postons sur Internet est d'une façon ou d'une autre utilisable et pistable mais nous n'y pouvons rien parce que nous n'y connaissons pas grand-chose. Allah ghaleb, les Algériens ne sont que des consommateurs dans tous les domaines !
- On se confie sur des forums, mais sous un pseudonyme. Cela ne suffit-il pas pour se protéger ? s'interroge une lycéenne.
- Même si on est « pisté » les jeunes ne peuvent pas déserter les réseaux sociaux sinon ils s'excluraient de fait d'une vie communautaire très puissante et solidaire, avec tous ses programmes ses invitations, ses organisations de fêtes, de sorties, de travail et surtout ses riches discussions entre copains, affirme une psychologue.

Si les internautes aiment échanger et partager en ligne c'est tout simplement parce qu'ils en tirent des satisfactions :

- Je n'ai aucune autre alternative m'offrant les avantages que je trouve sur Internet. Quant aux risques concernant ma vie privée, bof on court des risques partout, même loin d'Internet, synthétise un étudiant.
- Pour ma part, les réseaux sociaux ne sont pas utilisés ; au fond pour « espionner » la vie privée des internautes, mais au contraire pour raconter sa vie publique, sa vie sociale. Les réseaux sociaux font partie de notre vie privée et sociale, en tout cas en ce qui me concerne et donc ma génération, nous confie une étudiante en post-graduation.

La maitrise de la technologie

Il est vrai que tous les internautes ne maitrisent pas les moyens techniques pour protéger la confidentialité des informations qu'ils publient ; de même qu'il leur est impossible de savoir qui peut avoir accès à leurs informations personnelles.

- Nous, les Algériens nous ne prenons pas le temps de lire tout ce qui se rapporte aux paramètres de confidentialité, du coup, nous divulguons et laissons nos coordonnées sans savoir que d'autres peuvent y avoir accès. Heureusement que chez nous, il n'y a pas encore de risques comme il en existe en France, par exemple, où on peut vous subtiliser votre numéro de carte bancaire…
- Nos paroles ont été plusieurs fois déformées à force d'être rapportées par les uns et les autres à une vitesse grand V. On arrive, à la fin du message à lire des « trucs » mais totalement faux ! soutient un jeune.
- Nous, les jeunes filles, nous contrôlons parfaitement les informations que nous devons publier parce justement nous ne maîtrisons pas l'outil technologique et informatique. Nous craignons énormément que des voisins ou des connaissances parlent de nous.
- Essentiellement d'âge mûr, cette catégorie de personnes interrogées se connectant de temps en temps s'intéressent peu à Internet et encore moins aux réseaux sociaux. En outre, elles ne savent pas particulièrement surfer sur internet ; elles ont donc peur de s'aventurer sur un terrain presque inconnu. Elles s'abstiennent ainsi de diffuser leurs informations et leurs coordonnées.

Synthèse : Au terme de notre enquête, nous notons qu'une majorité des internautes interrogés se sent démunie en termes de protection de leur vie privée sur Internet et aujourd'hui, ils s'interrogent sur l'utilisation de leurs données personnelles en ligne.

Un très faible nombre des répondants déclarent lire une toute petite partie les conditions d'utilisation et de confidentialité. D'ailleurs, ils soutiennent que ces textes trop longs sont difficiles à comprendre.

Aujourd'hui, les internautes, tout âge confondu, se disent inquiets de l'usage qu'ils font d'Internet et des informations qu'ils y laissent. Pour autant, ils continuent à surfer sans se préoccuper des problèmes qu'ils pourraient rencontrer. Ils adoptent donc un comportement passif, cependant, ils diffusent de moins en moins d'informations.

Les jeunes semblent mieux maîtriser ce qu'ils publient. Ils sont plus ouverts car ils tiennent en partie les manettes de leur outil technologique. Ces citoyens numériques savent comment effacer leurs traces de navigations.

Quant aux aînés qui ne maîtrisent pas l'outil informatique ou qui sont dépassés par ces enjeux comme ils craignent de tomber dans les écueils, ils évitent autant que faire se peut de publier des informations les concernant.

Pour conclure : Les conclusions de notre enquête présentent l'image d'une génération de personnes qui attachent beaucoup d'importance à Internet en tant qu'outil de travail et qui pensent contrôler l'utilisation qu'elles en font. Parallèlement, les conclusions dépeignent une génération plus jeune qui connait le monde des communications sur Internet comme un lieu hors de la portée et des connaissances des parents. De toute évidence, chez ces jeunes, en particulier les adolescents, Internet a agrandi le fossé existant entre eux et leurs parents.

Les réseaux sociaux permettent de rapprocher les gens de toutes catégories sociales, raciales, professionnelles... Cependant, certains se dévoilent tellement qu'ils se retrouvent presque « nus » sur la Toile.

Enfin, l'internaute a tendance à oublier la valeur du réel et du contact humain avec le monde virtuel. Il préfère se poster durant des heures devant son ordinateur à clavarder avec ses amis virtuels plutôt que de voir le vrai monde extérieur, vivre et passer son temps avec sa propre famille.

Bibliographie

Bera, Michel & Mechoulan, Eric 1999. *La machine Internet,* Paris Editions Jacob.

Levy, Alain. 2010. *Sur les traces de Big brother : la vie privée à l'ère numérique* Paris, L'Editeur.

Manach, Jean-Marc. 2010. *La vie privée, un problème de vieux cons* ? Paris, Fyp.

Nathan, Fernand 1979. *Informatique et vie privée,* Bruxelles, Labor.

Rey, Bénédicte. 2012. La vie privée à l'ère du numérique, Paris, Hermès science publications.

Tannier, Xavier. 2010. *Se protéger sur Internet : conseils pour la vie en ligne*, Paris Eyrolles.

Unesco. 2005. *Les droits de l'homme dans le cyberespace*, Paris, Economica.

Techniques de la Reconnaissance Automatique de la Parole, Application pour la langue arabe

M. Zaidi Amar
Département de génie industriel Université de Batna

ملخص: الهدف الرئيسي من هذا العمل هو ايجاد نقطة انطلاق، من أجل إنشاء نظام للتعرف التلقائي للكلام، خاص باللغة العربية، معتمدين في انشائه على نطاق كامل مخصص للتطبيقات الخاصة بألة التعلم.

الطريقة المعتمدة في هذا النظام تسمى نماذج ماركوف الخفية (*MMC* بالفرنسية أو *HMM* بالانجليزية).

كلمات مفتاحية: المعرفة التلقائية للكلام، النموذج الصوتي، نماذج ماركوف الخفية.

Résumé* : *Le but de ce travail est de fixer un point de départ, en vue de la réalisation d'un système de la Reconnaissance Automatique de la Parole pour la langue arabe, ce système est basé sur l'utilisation d'un Framework[i] complet pour le développement des applications Machine-Learning.

La méthode adoptée pour la reconnaissance est dite les modèles de Markov cachés (MMC, en Anglais HMM)

Mots clefs — Reconnaissance automatique de la parole (RAP) Modèle acoustique, HMM.

Introduction

La reconnaissance automatique de la parole (RAP) consiste à extraire, à l'aide d'un ordinateur, l'information lexicale contenue dans un signal de parole.

Les fondements de la technologie récente en reconnaissance de la parole ont été élaborés par F. Jelinek et son équipe à IBM dans les années 70 [1]. Les applications qui ont peut imaginer sont nombreuse : aider les personnes handicapées, contrôle vocal des machines réservation des vols, apprentissage d'autres langues, etc [2].

Vue de l'importance de la RAP, plusieurs systèmes ont été développés pour la reconnaissance vocale, parmi ces systèmes on trouve le HTK [3], et Sphinx.

Les modèles de la RAP continue

Pour arriver à une reconnaissance automatique de la parole continue, on doit passer par quatre modules, le premier est le traitement de signal audio, il consiste à segmenter le signal audio en un ensemble fini d'unités primitives, puis on passe au module acoustique, qui faire reconnaître la sémantique de chaque unité « mot phonème ou syllabe», avec des résultats multiples pour chaque unité.

Le module lexical, intégré avec le module syntaxique nous permettre de rassembler les bonnes sorties du module acoustique pour construire la phrase ou le mot prononcé.

En résumant, la reconnaissance automatique de la parole continue passe par deux principaux modèles dits « modèle acoustique & modèle de la langage ». *Fig.1.*

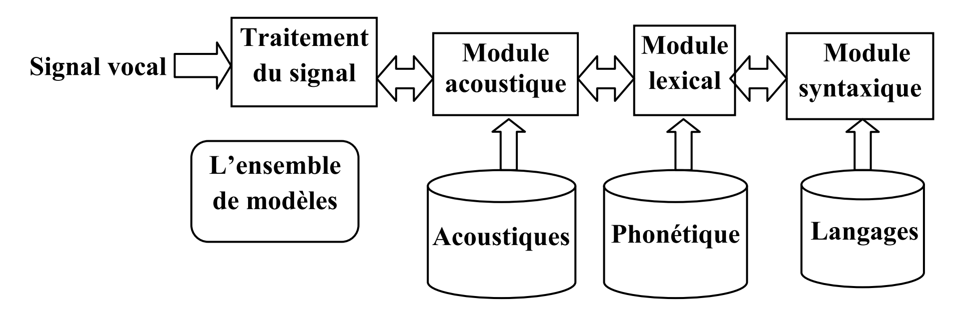


Fig.1 Architecture globale d'un Système de Reconnaissance de la parole

Modèles acoustiques

A. Du signal aux vecteurs acoustiques :

Le signal de parole ne peut être exploité directement. En effet, il contient non seulement le message linguistique, mais aussi de nombreux autres éléments comme des informations liées au locuteur aux conditions d'enregistrement, etc. Toutes ces informations ne sont pas nécessaires lors du décodage de parole et rajoutent même du bruit. De plus, la variabilité et la redondance du signal de parole le rendent difficilement exploitable tel quel.

Il est donc nécessaire d'en extraire uniquement les paramètres qui seront dépendants du message linguistique. Ces paramètres sont estimés via des fenêtres glissantes sur le signal. Cette analyse par fenêtrage permet d'estimer le signal sur une portion jugée quasi-stationnaire, généralement 10 à 20 ms, en limitant les effets de bord et les discontinuités du signal via une fenêtre de Hamming [4].

B. Modélisation acoustique à base de modèles de Markov cachés

Concernant la modélisation statistique acoustique, « F. Jelinek & J. Baker » [1] [5], introduisent les modèles de Markov cachés (Hidden Markov Model, HMM) dans ce domaine. Ces modèles sont aujourd'hui utilisés dans un très grand nombre des systèmes de reconnaissance automatique de la parole.

Chaque unité acoustique, en effet, est modélisée par un chaine de Markov cachée. Dans le cas de petits lexiques, ces unités peuvent être les mots. Dans le cas de grands lexiques, l'unité préférée est le phonème (ou polyphone) ce qui limite le nombre de paramètres à estimer.

C. Dictionnaire de prononciation

Le dictionnaire de prononciation (ou dictionnaire phonétique) fournit le lien entre les séquences des unités acoustiques et les mots représentés dans le modèle de langage. Il est important de noter que les performances du système de reconnaissance sont directement liées au taux de mots hors vocabulaire. Bien qu'un dictionnaire de prononciation créé manuellement permette une bonne performance, la tâche est très lourde à réaliser et demande des connaissances approfondies sur la langue en question. En plus, les noms propres sont l'un des problèmes majeurs pour toutes les langues. Par exemple, les 20 000 noms propres inclus dans le dictionnaire anglais COMPLEX ne représentent qu'une petite fraction des un à deux millions de noms rassemblés par « X. Huang »[6] sur des données en anglais US.

D. Décodage acoustico-phonétique

un décodage acoustico-phonétique (DAP) est défini comme la transformation de l'onde vocale en unités phonétiques ; c'est une sorte de transcodage qui fait passer d'un code acoustique à un code phonétique ou plus exactement comme la mise en correspondance du signal et d'unités phonétiques prédéfinies pour lequel le niveau de représentation passe de continu à discret. Le décodage acoustico-phonétique est composé d'une première partie consistant à extraire les

paramètres acoustiques et à les représenter sous forme de vecteurs acoustiques à partir du signal à décoder, et d'une seconde partie qui, à partir de ces jeux de paramètres, apprend des modèles d'unités acoustiques ou décode le signal d'entrée, selon que l'on veuille apprendre ou reconnaître[7].

Modèles de langage

Dans l'équation bayésienne appliquée à la reconnaissance automatique de la parole apparaît une probabilité a priori de la séquence. Cette probabilité se calcule à partir d'un modèle de langage. Ainsi, la séquence « je suis ici » est plus probable, en terme de langage, que « jeu suis ici », ou encore «jeux suit y si », bien que l'acoustique soit quasi-similaire. Pour une même suite de phonèmes, il peut exister plusieurs dizaines de phrases possibles. Le rôle principal du modèle de langage est de les classer selon leur plausibilité linguistique.

Évaluation des systèmes de reconnaissance de la parole

Les systèmes de reconnaissance de la parole sont évalués en terme de taux de mots erronés (WER : Word Error Rate). Généralement, il y a trois types d'erreurs sur les mots reconnus par le système de reconnaissance de la parole :

- substitution (Sub) ou remplacement du mot correct par un autre mot.
- suppression (Sup) ou omission d'un mot correct.
- insertion (Ins) ou ajout d'un mot supplémentaire.

Ces trois types d'erreur peuvent être calculés après alignement dynamique entre l'hypothèse du décodeur et une transcription de référence, [4] à l'aide d'un calcul de distance d'édition minimale entre mots. Le résultat sera le nombre minimal d'insertions, de substitutions et d'élisions de mots, pour pouvoir faire correspondre les séquences de mots de l'hypothèse et de la référence. D'après sa définition, le WER peut être supérieur à 100 % à cause des insertions.

$$\text{WER} = \frac{\text{nb sub} + \text{nb de sup} + \text{nb de ins}}{\text{nb de mots correct}} \quad (1)$$

Quelques outils de la reconnaissance automatique de la parole

A. HTK

Hidden Markov Model Toolkit (HTK) est un ensemble d'outils portable permettant la création et la manipulation de modèles de

Markov cachés. HTK est principalement utilisé dans le domaine de la recherche de la reconnaissance vocale bien qu'il soit tout à fait utilisable dans de nombreuses autres applications telles que la synthèse vocale, la reconnaissance de l'écriture ou la reconnaissance de séquences d'ADN.

Il est composé d'un ensemble de modules et outils écrits en langage C. Ces différents outils facilitent l'analyse vocale, l'apprentissage des HMM, la réalisation de tests et l'analyse des résultats. Il est à noter que ce qui a contribué au succès de HTK, est qu'il est accompagné d'une assez bonne documentation.

B. Sphinx 4

Sphinx 4 est un logiciel de reconnaissance vocale écrit entièrement en Java. Les buts de Sphinx sont d'avoir une reconnaissance vocale hautement flexible, [8] d'égaler les autres produits commerciaux et de mettre en collaboration les centres de recherche de diverses universités.

Tout en étant hautement configurable, la reconnaissance de Sphinx 4 supporte notamment les mots isolés et les phrases (utilisation de grammaires). Son architecture est modulable pour permettre de nouvelles recherches et pour tester de nouveaux algorithmes.

La qualité de la reconnaissance dépend directement de la qualité des données vocales. Ces dernières étant les informations relatives à une voix propre. Ce sont par exemple les différents phonèmes, les différents mots (lexique), les différentes façons de prononciation. Plus ces informations ne seront importantes et connues par le système meilleure sera sa réaction et ses choix à faire.

Les caractéristiques du son

Le son est défini par trois paramètres acoustiques : l'intensité, la fréquence et la durée.

- ✓ L'intensité :

Elle est définie par le Dictionnaire d'Orthophonie (2004) comme «la puissance du son, de la voix, mesurée en décibels (dB) grâce à un sonomètre».

- ✓ La fréquence :

Elle correspond au « nombre de vibrations par seconde d'un son pur périodique déterminant sa hauteur physique » (Ibid.). Plus la fréquence d'un son est élevée, plus ce son est aigu. La fréquence se mesure en Hertz (Hz).

✓ La durée :

La durée se définit comme l’intervalle séparant deux évènements. Selon Lienard (cité par « G. Laboulais 2007 » [9], un événement sonore dure au moins soixante millisecondes pour être perçu par l’oreille.

Ces trois paramètres composent le signal acoustique. Leur traitement par le système auditif permet notamment de reconnaître et d’identifier une source sonore, de la localiser dans l’espace, de décoder la parole et d’en analyser la prosodie [9]. Une représentation courante est l'amplitude de l'onde en fonction du temps :

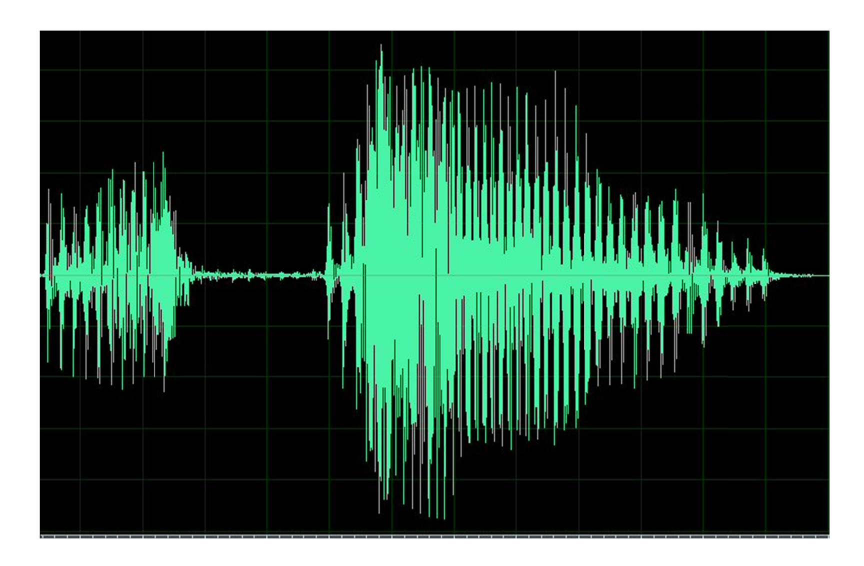


Fig.2 Représentation bidimensionnelle du son.

Analyse et traitement de la parole :

Il existe plusieurs méthodes d’analyse qui sont utilisés en vue de la reconnaissance de la parole.

- ***Energie du signal*** : Le paramètre intuitif pour caractériser le signal ainsi obtenu est l’énergie. Cette énergie correspond à la puissance du signal. Elle est souvent évaluée sur plusieurs trames de signal successives pour pouvoir mettre en évidence des variations [10]. La formule de calcul de ce paramètre est :

$$E_N = \sum_{n=0}^{N-1} S(n)^2$$

S (n) : signal parole échantillonné.

- ***Taux de passage par zéro*** : Le taux de passage par zéro (zero crossing rate) représente le nombre de fois que le signal, dans sa représentation amplitude/temps, passe par la valeur centrale de l'amplitude (généralement zéro). Il est fréquemment employé pour des algorithmes de détection de section voisée/non voisée dans un signal.
- ***Analyse cepstrale*** : L'analyse cepstrale résulte du modèle de production, son but est d'effectuer la déconvolution (source/ conduit) par une transformation homomorphique: les coefficients sont obtenus en appliquant une transformée de Fourier numérique inverse au logarithme du spectre d'amplitude. Le signal ainsi obtenu est représenté dans un domaine appelé cepstral ou quérulent ; les échantillons se situant en basses fréquences correspondent à la contribution du conduit vocal et donnent les paramètres utilisés en RAP, tandis que la contribution de la source n'apparaît qu'en hautes fréquences.

Reconnaissance Automatique de la Parole « chiffres arabe »

Le système développé, appartient au modèle acoustique, où les unités phonétiques à reconnaître sont les chiffres arabes, avec une base de connaissance crée, en utilisant un simple microphone. En enregistrant les mots correspondants aux chiffres et avec une analyse et un traitement pour chaque mot, on extraire les paramètres caractéristiques des mots « par une analyse cepstrale dite MFCC, les coefficients de Mel » vers la base de connaissance.

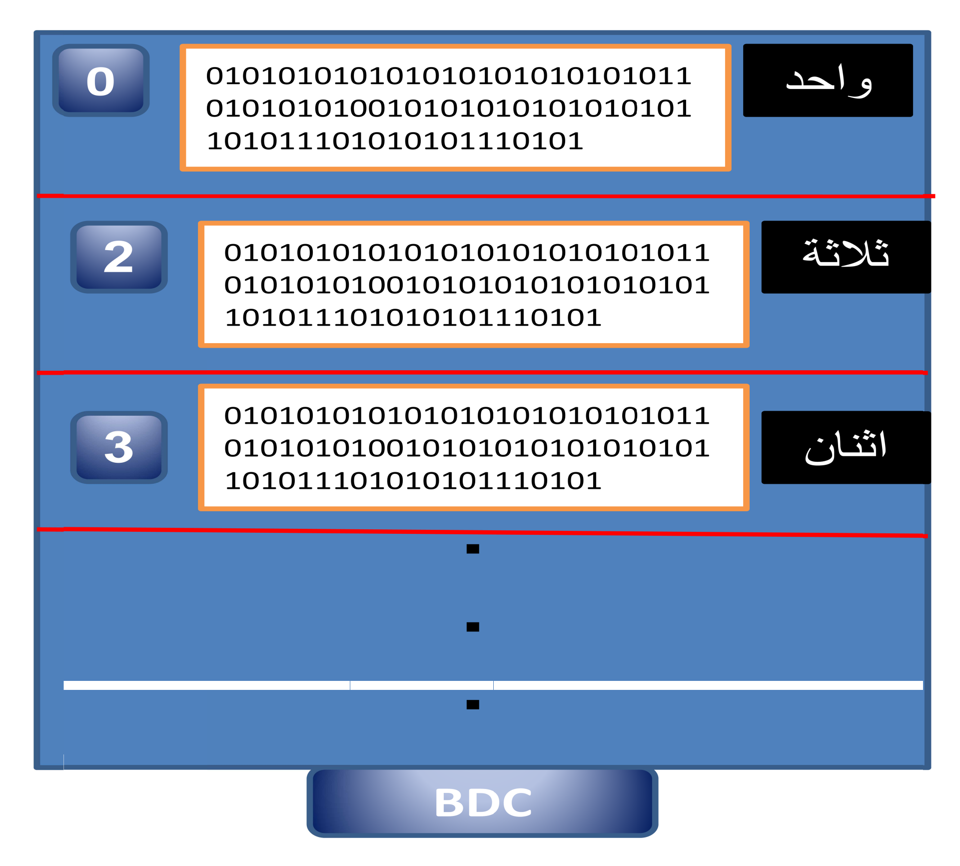


Fig.3 Représentation de la base de connaissances.

Après la création de la base de connaissance on passe à la phase de la reconnaissance des chiffres, cette fois-ci le locuteur passe le chiffre à reconnaitre par le microphone et le système va extraire ses paramètres caractéristiques et les compare aux données des unités de la base de connaissance, en utilisant les modèles de Markov cachés, le système décide l'unité la plus probable parlée par le locuteur.

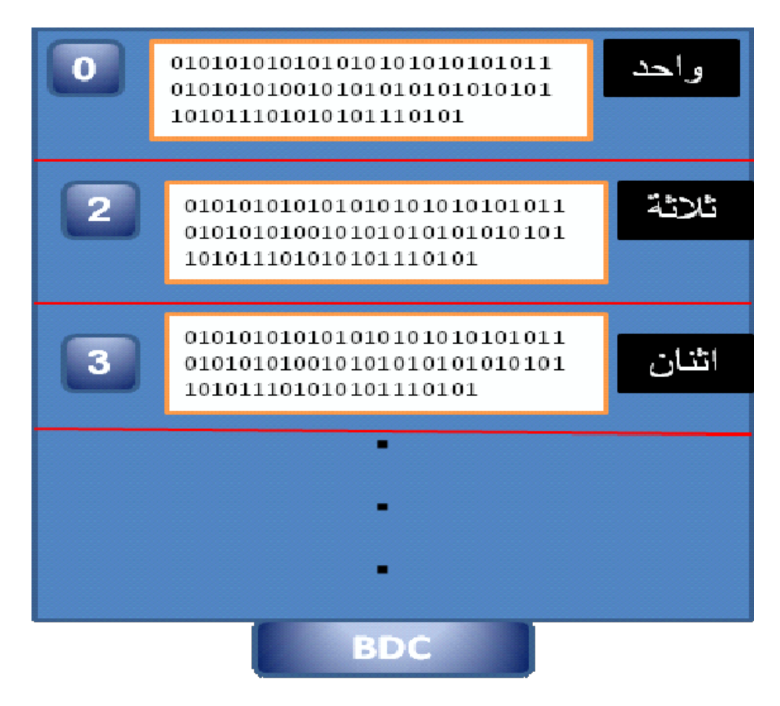


Fig.4 la reconnaissance d'un mot.

Résultats de l'expérimentation

	Masculins (07)	Féminins (05)
صفر	20%	30%
واحد	50%	40%
اثنان	54%	50%
خمسة	60%	54%
سبعة	20%	10%
ستة	15%	10%
تسعة	10%	15%

Tab1 pourcentage de la reconnaissance.

Conclusion et perspectives :

Les résultats de la reconnaissance, dans le cas de la langue arabe n'ont été pas très efficaces à cause de l'absence d'une connaissance préalable de la syllabification arabe, dont on espère d'avoir une forte collaboration avec les linguistes arabe.

Références

[1] F. Jelinek & C. Nom2, "*Continuous speech recognition bystatistical methods*," *Proceedings of the IEEE,* 1976, PP 532-556.

[2] "http://fr.wikipedia.org/wiki/Reconnaissance_vocale".

[3] "http://htk.eng.cam.ac.uk".

[4] S.Seng, "*Vers une modélisation statistique multi-niveau du langage,*" L'Université de Grenoble,France,2010.

[5] J. Baker," *Stochastic Modeling for Automatic Speech understanding,*" Academic Press,New York,1975, PP 521-542.

[6] X. Huang & A. Acero & H. Hon, "*Spoken language processing,*" Prentice Hall PTR Upper Saddle River, NJ, USA, 2001.

[7] J. Haton & J. Pierrel & G. Pérennou & J. Caelen & J. Gauvain, " *Reconnaissance automatique de la parole* ," Dunod,1991.

[8] Philippe Galley, Blaise Grand & Samuel Rossier, "*Logiciel de reconnaissance vocale Sphinx-4,*" Ecole d'ingénieurs et d'architectes de Fribourg, 2006.

1-Framework **:** est un ensemble cohérent de composants logiciels structurels, qui sert à créer les fondations ainsi que les grandes lignes de tout ou d'une partie d'un logiciel (architecture)**.**

Les ressources de protection contre les menaces de la sécurité des systèmes d'information

Melle Galleze Hadjila
Université Mouloud Mammeri de Tizi-Ouzou

الملخّص باللّغة العربيّة: تعتبر المؤسّسة البدن الاجتماعي الحي، كما أنّ دوران المعلومة فيها هو قطب النّهج التّنظيمي لها وكأنّها دم هذا البدن أي العنصر الحيوي لها؛ لتبقى هذه الأخيرة كبلاغ أو كرسالة للمرسل إليه (المخاطَب)؛ لتعبّر عن علمه ومدى معرفته بموضوع ما لتسمح بحل المشكلة، فهي إذن معطى الحقل الدّراسي الّذي يلحق به مدلول واضح لمختلف عمال المنظّمة، وبالتّالي تلعب دور ضروريّ في سير أخذ القرار، ولتحسين جمع انتقال ومعالجة المعلومة تعمد المؤسّسة لتسأل عن تنظيمها المعلوماتي؛ لأنّ علم تقنيّة المعلومات يشجّع نمو وإبراز قيمتها أكثر بالمؤسّسة، والّتي بدورها لها قيمة باطنيّة تكمن في مدى مبادلتها وتقسيمها لها كونها تحيل هذه القيمة بمساعدة الشركاء والمتعاونين على التّصرّف بها بكل فاعليّة أثناء البحث في تحقيق الأهداف المنشودة والمقرّرة به، وذلك عن طريق تطوير وتنميّة استخدام الإنترنيت، وبواسطتها تفتح المؤسّسة أنظمتها المعلوماتيّة لممموليها وشّركائها، فمن الضّروري جدا معرفة مواردها الواجب حمايتها بالفعل، وأيضا معرفة إتقان ومراقبة الدّخول إليها، وحق استخدام تنصيب مستخدمي النّظام المعلوماتي؛ لذا حاولنا في مداخلتنا هذه اقتراح حلول ممكنة التّصدي للمخاطر والمشاكل الّتي تواجهها الأنظمة المعلوماتيّة داخل المؤسّسة.

Introduction :

En considérant que l'entreprise est un corps social vivant, et comme la circulation de l'information c'est le pivot du système

organisationnel de l’entreprise, alors l’information est le sang de ce corps social tant qu’elle est son élément vital. En effet l’information est un message perçue par un destinataire, qui modifie sa connaissance sur un sujet ou qui lui permet de résoudre un problème. Ainsi qu’elle est une données du domaine d’étude qui associé un **sens** compréhensible des différents acteurs de l’organisation. Encore l’information a surtout un rôle essentiel dans le processus de **prise de décision** tant au niveau des décisions opérationnelles quotidiennes qu’au niveau des grandes décisions stratégiques. Fort heureusement, les entreprises sont de plus en plus nombreuses à s’interroger sur leur organisation informationnelle, à améliorer la collecte, la circulation et le traitement de l’information. Ainsi que Les technologies de l'information favorisent l'augmentation de la valeur de l'information pour les entreprises. Et si l'information a une valeur intrinsèque, Alors elle développe cette valeur dans son échange et son partage. En effet l'information **acquiert de la valeur** quand elle aide les collaborateurs à agir plus efficacement lorsqu'ils cherchent à réaliser les objectifs qui leur sont assignés par l'entreprise.

Avec le développement de l’utilisation de l’internet, les entreprises ouvrent leur système d’information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaitre les ressources de l’entreprise à protéger et de maitriser le contrôle d’accès et les droits des utilisateurs du système d’information. Et pour qu'une information puisse être exploitée dans une entreprise ou dans la prise de décision ; elle doit respecter un certain nombre de qualité à savoir : la pertinence, la disponibilité, le cout raisonnable, et la fiabilité.

Durant ce travail on s’intéresse à la qualité ***fiabilité*** qui représente que l’information est vraie, précise, et à jour. En fait pour garantir cette qualité un processus plus important est nécessaire, ce processus s’agit de la ***sécurité de l’information*** qui vise généralement cinq objectifs qui sont ***: l’intégrité***, ***la***

confidentialité, ***la disponibilité***, ***la non répudiation*** et **l'authentification**.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaitre la façon de procéder de l'ennemi. Et puisque l'avènement de l'informatique a introduit une forme numérique de données enregistrées sur des supports électroniques et comme les ordinateurs sont de plus en plus omniprésents et le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, Alors au niveau de la recherche, la sécurité des systèmes d'information a principalement été traitée par les sciences de l'informatique.

Par conséquent, le thème de notre séminaire est consacré sur la sécurité informatique, en considérant que la sécurité de l'information possède plusieurs domaines. D'ailleurs le but de cette intervention est de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions. Puisque une menace informatique représente le type d'actions susceptibles de nuire dans l'absolu à un système informatique, et comme elle peut être le résultat de diverses actions en provenance de plusieurs origines: ***Origine opérationnel***, ***origine physique***, ***origine humaine***. Des ressources de protection contre ces menaces ont été mise en place.

Durant ce travail on va aborder ces ressources de protection après avoir identifié les menaces. Le travail est organisé selon trois parties en commençant par la sécurité de l'information en visant ses objectifs et ses domaines, ensuite les menaces informatiques en les identifiants et précisant leurs origines, et enfin les ressources de protection contre ses menaces. ***Quels sont alors les ressources de protection contre les menaces de la sécurité des systèmes d'information ?***

I. **La sécurité de l’information :** L’information est des renseignements consignés sur un support quelconque, dans un but de transmission des connaissances. Une information quel que soit son canal de communication ou son support, elle doit être en mesure de sécurité. En effet, la sécurité de l’information est un Moyen concret assurant, partiellement ou totalement, la protection d’un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent. La sécurité de l’information n'est confinée ni aux systèmes informatiques, ni à l'information dans sa forme numérique ou électronique. Mais, elle s'applique à tous les aspects de la sureté, la garantie, et la protection d'une donnée ou d'une information, quelle que soit sa forme. Encore elle ne peut pas être définie comme synonyme de la sécurité informatique, de la sécurité système et réseau, de la sécurité des technologies de l’information, de la sécurité du système d’information, ou de la sécurité des technologies de l’information et de la communication. Chacune de ces expressions traite un sujet différent, même si le point commun concerne la sécurité de l'information ; par conséquent, tous sont des sous-domaines de la sécurité de l'information. [1]

La sécurité de l'information est donc un domaine vaste et fait partie des tâches importantes de chaque cadre, dans chaque entreprise ou chaque organisation. Mais la sécurité de l’information sur laquelle notre séminaire est porté est celle qui fait partie des domaines d’application de la sécurité informatique, est alors la sécurité des systèmes d’information.

I. 1. La sécurité informatique :

La sécurité est la situation dans laquelle un système informatique, connecté ou non à un réseau externe de télécommunications, est protégé des dangers internes ou externes. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

«La sécurité informatique est l'ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information ».[2]

Encore, « elle est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles ».[3]

Autrement dit la sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des ressources possèdent uniquement les droits qui leur ont été octroyés. Ainsi que la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leurs sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

I. 1. 1.Les domaines d'application de la sécurité informatique :

Puisque le système d'information est un élément absolument vital pour toute organisation, et représente encore *un patrimoine essentiel de l'organisation, qu'il convient de protéger alors* la sécurité des systèmes d'information (SSI) est une discipline de première importance. Et comme tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information sachant qu'est un ensemble organisé de ressources (les personnels, le matériel, les logiciels, les procédures) qui permet de collecter, stocker, traiter et diffuser de l'information. Donc la sécurité informatique se décline en:

- **sécurité physique et environnementale** : Cette sécurité mérite d'être systématiquement prise en compte dans le cadre de la politique de sécurité des organisations afin de garantir la protection physique de leurs données. La sécurité physique

concerne tous les aspects liés à l'environnement dans lequel les systèmes se trouvent, donc elle repose essentiellement sur :

- la protection de l'environnement (mesures ad hoc notamment pour faire face aux risques d'incendie, d'inondation ou encore de tremblement de terre… pour respecter les contraintes liées à la température, à l'humidité, etc.) ;
- la protection des sources énergétiques et de la climatisation (alimentation électrique, refroidissement, etc.) ;
- Protection des accès par des mesures de gestion et de contrôle des accès physiques aux locaux, équipements et infrastructures (avec entre autres la traçabilité des entrées et une gestion rigoureuse des clés d'accès aux locaux).
- La redondance physique (des infrastructures et sources énergétiques) ;
- l'usage d'équipements qui possèdent un bon degré de sûreté de fonctionnement et de fiabilité ;
- le marquage des matériels pour notamment contribuer à dissuader le vol de matériel et éventuellement le retrouver ;
- le plan de maintenance préventive (tests) et corrective (pièces de rechange) des équipements ce qui relève également de la sécurité de l'exploitation des environnements.

➢ **Sécurité de l'exploitation :** renferme tout ce qui touche le bon fonctionnement des systèmes informatique, elle comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour.

➢ **Sécurité logique :** Fait référence à la réalisation de mécanisme de sécurité par logiciel en contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données. Elle repose généralement sur :

✓ Dispositifs pour garantir la confidentialité et l'intégrité grâce à la procédure cryptographie.

✓ Le contrôle d'accès et la gestion efficace des mots de passe, par authentification.

✓ La maintenance préventive, par les mesures de sauvegarde, antivirus et tests de sécurité.

➢ **sécurité applicative et sécurité de l'information:** Le principe de la sécurité applicative consiste au développement pertinent des applications ainsi que leur intégration et exécution harmonieuses dans l'environnement opérationnelles. Elle repose essentiellement sur un ensemble de facteur tel que : les méthodes de développement, la robustesse des applications, tests et assurance de sécurité, les contrôles programmés,…

☞ **La protection de l'information** revient à comprendre son rôle, son importance stratégique et l'impact des décisions qui la concernent. Et consiste à assurer son **exactitude** et sa **pérennité** pour le temps nécessaire à son exploitation et à son archivage. Cela oblige de déterminer le niveau de protection nécessaire aux informations manipulées, par une classification des données qui permet de qualifier leur degré de sensibilité (normale confidentielle) et de les protéger en fonction de ce dernier.

➢ **sécurité des infrastructures informatique et de télécommunication :**

Repose sur le principe d'offrir à l'utilisateur final une connectivité fiable et de qualité de « bout en bout », donc elle consiste à mettre un canal de communication fiable entre les correspondants, quels que soient le nombre et la nature des éléments intermédiaires. Cela passe par la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements.[4] Voici maintenant le schéma qui représente la sécurité informatique globale.



Figure1 : Domaines de la sécurité informatique.

I. 1.2. Les objectifs de la sécurité informatique:

La sécurité informatique vise généralement cinq objectifs principaux qui sont :

1) La disponibilité :

Une ressource doit être accessible, avec un temps de réponse acceptable.

Encore la disponibilité de cette ressource est indissociable de sa capacité à être **accessible** par l'ensemble des ayants droit. Par conséquent la disponibilité des services, systèmes, et données est obtenue par un **dimensionnement approprié** et une gestion opérationnelle des ressources et des services.

2) Intégrité :

Certifier que les données, les traitements ou les services :

- N'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.
- N'ont pas été modifiées lors de leur stockage ou de leur transfert.
- Sont protégées des écoutes actives qui peuvent modifier les données interceptées. [5]

3) Confidentialité :

La confidentialité est le maintien du secret des informations et peut être vue comme la *« protection des données contre une divulgation non autorisée».* Elle se base donc sur :

- Protection des données contre une divulgation non autorisée.
- Limitation des accès par un mécanisme de contrôle d'accès (procédure d'authentification).
- Transformation des données par des procédures de chiffrement (Cryptographie). [6]

4) Authentification et identification :

Faire identifier l'auteur d'un document peut être aisé, par contre mettre en place des mesures de sécurité pour assurer l'authenticité du document est chose plus délicate. Ainsi ces mesures assurent :

- Confidentialité et intégrité : seuls les ayant droit peuvent accéder aux ressources.
- Non-répudiation et imputabilité : preuve de l'origine d'un message, d'une transaction, preuve de la destination. [7]

5) Non répudiation :

La non-répudiation consiste à ne pas pouvoir nier ou rejeter qu'un évènement a eu lieu.

A cette notion sont associées :

L'imputabilité: une action a eu lieu et automatiquement un enregistrement, preuve de l'action, est effectué.

La traçabilité: mémorisation de l'origine du message. Permet de suivre la trace numérique laissée par la réalisation d'un évènement (message électronique, transaction commerciale transfert de données…).

L'auditabilité: capacité d'un système à garantir la traçabilité des accès et des tentatives d'accès et la conservation des ces traces comme preuves exploitables.

I. 2. <u>La sécurité des systèmes d'information</u> :

L'information se présente sous trois formes : les données, les connaissances et les messages. Et par système d'information on

désigne l'ensemble des moyens techniques et humains qui permet de stocker, de traiter ou de transmettre l'information. Et comme les moyens informatiques, électroniques et la télécommunication sont largement utilisés pour automatiser et dématérialiser les opérations d'entreprises en lieu des moyens classiques tels que les formulaires sur papier et le téléphone et cette transformation est à l'origine de la notion de système d´information. Et sachant que, cette automatisation de traitement de l'information est l'objectif d'un système informatique tant qu'il est ensemble des moyens informatiques et de télécommunication ayant pour finalité d'élaborer, traiter, stocker acheminer, présenter ou détruire des données. On dira donc qu'un système d'information est *«tout moyen dont le fonctionnement fait appel d'une façon ou d'une autre à l'électricité et qui est destiné à élaborer, traiter, stocker acheminer, présenter ou détruire l'information ».* Et donc la sécurité des systèmes d'information recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un système d'information et elle repose essentiellement sur trois critères qui sont : [8]

– ***La disponibilité des services :*** les services (ordinateurs réseaux, périphériques, applications…) et les informations (données, fichiers…) doivent être accessibles aux personnes autorisées quand elles en ont besoin. Donc est une propriété d'accessibilité au moment voulu par les utilisateurs autorisés.

– ***La confidentialité des informations :*** les informations n'appartiennent pas à tout le monde ; seuls peuvent y accéder ceux qui en ont le droit ; Cette propriété dit que l'information n'est ni disponible ni divulguée aux non autorisés.

– ***L'intégrité des systèmes :*** C'est la prévention d'une modification non autorisé de l'information.

☞ Le schéma ci-dessous nous présente ces trois critères sous format d'un triangle :

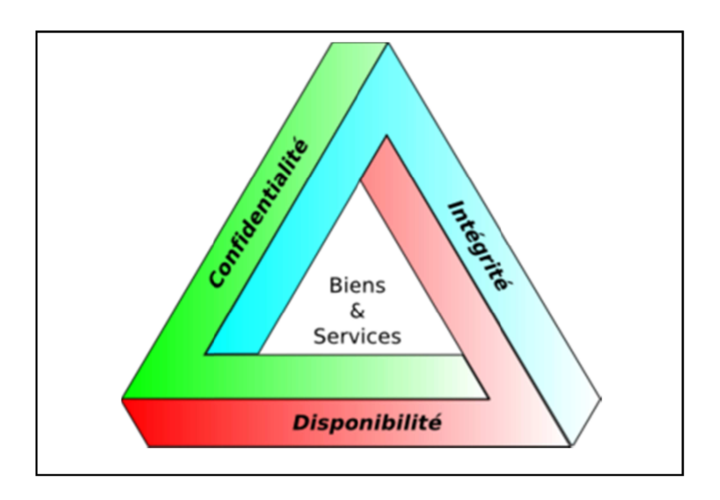


Figure2 : Représentation de la triade **D, I** et **C**

II. Les menaces contre la sécurité des systèmes d'information :

« L'information gérée par les systèmes d'information fait l'objet de convoitises. Elle peut être exposée à des attaques qui exploitent des éléments vulnérables du système d'information. La sécurité des systèmes d'information a pour objet de contrer ces menaces par des mesures proportionnées aux risques pouvant peser sur la confidentialité de l'information, son intégrité, sa disponibilité ou la possibilité d'en authentifier la source et de la signer ».[9] Et pour atteindre ces objectifs de sécurité, il est nécessaire de mettre en œuvre une politique de sécurité, et Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaitre la façon de procéder de l'ennemi. Une menace informatique représente le type d'actions susceptibles de nuire dans l'absolu à un système informatique, et elle peut être le résultat de diverses actions en provenance de plusieurs origines. Quels sont alors ces origines ?

II. 1. Les origines des menaces :

- **Origine opérationnel:**

A l'origine opérationnel, les menaces sont liées à un état du système à un moment donné. Elles peuvent être le résultat d'un

bogue logiciel (Buffer Overflows, format string …etc.), d'une erreur de filtrage des entrées utilisateur (typiquement les XSS et SQL injection), d'un dysfonctionnement de la logique de traitement ou d'une erreur de configuration.

- **Origine physique:**

Les menaces dans ce cas peuvent être d'origine accidentelle naturelle ou criminelle. Et comme on ajoute encore les désastres naturels, les pannes ou casses matérielles, le feu ou les coupures électriques.

- **Origine humaine:**

Dans ce cadre les menaces sont associées aux erreurs humaines, que ce soit au niveau de la conception d'un système d'information ou au niveau de la manière dont on l'utilise. Ainsi elles peuvent être le résultat d'une erreur de conception ou de configuration comme d'un manque de sensibilisation des utilisateurs face au risque lié à l'usage d'un système informatique. Par conséquent, Les utilisateurs doivent prendre en compte de grandes précautions afin de réduire la possibilité d'offrir l'accès à un intrus et/ou la possibilité de tomber dans des erreurs de conception ou de configuration.

II. 2. Les causes de l'insécurité :

On distingue généralement deux types d'insécurité :

- **L'état actif d'insécurité**, c'est-à-dire la non-connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple la non-désactivation de services réseaux non nécessaires à l'utilisateur).
- **L'état passif d'insécurité**, c'est-à-dire lorsque l'administrateur (ou l'utilisateur) d'un système ne connait pas les dispositifs de sécurité dont il dispose.

II. 3. Identification des menaces contre la sécurité des systèmes d'information :

La sécurité des systèmes d'information fait partie intégrante de la sécurité globale et «La mise à exécution de menaces volontaires ou involontaires, humaines ou matérielles peut porter atteinte au SI, aux personnels et à l'organisme. Il convient de

distinguer ce qui relève **d'attaques délibérées (agressions)** et ce qui relève de **sinistres naturels** (incendie, explosion inondations…) ».[10] Donc les principales menaces effectives auxquelles un système d'information peut être confronté sont:

- Un utilisateur du système: C'est l'insouciance des utilisateurs généralement qui engendre la majorité des problèmes liés à la sécurité d'un système d'information.

- Une personne malveillante : une personne peut s'introduire sur le système, légitimement ou non, et va accéder ensuite à des données ou à des programmes auxquels elle n'est pas censée avoir accès. (La fonction des pirates).

- Un programme malveillant: un logiciel installé par mégarde ou par malveillance, destiné à nuire des ressources du système en ouvrant la porte à des intrusions ou en modifiant les données.

- Des données personnelles : peuvent être collectées à l'insu de l'utilisateur et être réutilisées à des fins malveillantes ou commerciales.

- Un sinistre (vol, incendie, dégât des eaux) : une mauvaise manipulation ou une malveillance entrainant une perte de matériel et/ou de données.

III. Les ressources de protection contre les menaces de la sécurité des systèmes d'information :

III. 1. Les besoins de sécurité :

Puisque un système d'information comprend :

- Les serveurs réseau et des postes de travail informatique (fixes et nomades);

- les applications (systèmes d'exploitation, suites bureautiques, logiciels métiers …;

- les infrastructures de communication et de télécommunication (réseaux locaux, liaisons intersites, réseau téléphonique, accès Internet, liaison radio …). Alors sa sécurité s'agit de protéger l'outil de travail (disponibilité), les données (confidentialité, disponibilité, intégrité), le personnel des unités et l'organisme.

III. 2. <u>Les ressources de protection</u> :

III. 2.1. <u>Formation des utilisateurs</u> :

En générale la majorité des problèmes de sécurité sont situés entre la chaise et le clavier d'un micro-ordinateur.

Discrétion: Les utilisateurs doivent avoir la sensibilisation envers la faible sécurité des outils de communication et envers l'importance du non divulgation d'informations par ces moyens. En effet, il est souvent trop facile d'obtenir des mots de passe par téléphone ou par e-mail en se faisant passer pour un membre important de la société.

Virus : D'après des études récentes 1/3 des utilisateurs étaient piégé par l'ouverture d'une pièce jointe d'un courrier nommée « I love You » et que la moitié étaient piégé par l'ouverture d'une pièce nommée « ouvrez-ça » ou similaire… ! Cette information est nécessaire, Donc attention aux rumeurs.

Charte: l'intérêt principal d'une charte d'entreprise est d'obliger les employés à lire et signer un document précisant leurs droits et devoirs et par la même de leur faire prendre conscience de leur responsabilité individuelle.

III. 2.2. <u>Protection de l'outil de travail</u> :

La disponibilité et l'intégrité de cet outil doivent donc impérativement être placées à l'abri de menaces internes ou externes. Et comme Le poste de travail reste un maillon faible de la sécurité. Le projet TCPA *(Trusted*

Computing Platform Alliance) a pour but d'améliorer sa sécurité en dotant le PC d'une puce dédiée à la sécurité. Elle sera chargée de vérifier l'intégrité du BIOS, du chargement de l'OS de sauvegarder les clés et certificats (PKI) et connaitra les protocoles de cryptage (RSA, DES…).

- Plusieurs cartes mères possèdent un cavalier interdisant la reprogrammation du BIOS (flashage), vérifier et mettre en place ce cavalier sur tous les postes!
- Lecteur de disquette : Interdire le Boot disquette (BIOS) voire inhiber complètement le fonctionnement du lecteur.

➢ Lecteur de CD-ROM : les virus de Boot sont très rares sur CD, mais avec la généralisation des graveurs et la simplification des logiciels de gravure…

➢ Backup régulier et sécurisé des informations essentielles.

➢ Multi-boot : à éviter au maximum car la sécurité globale du poste est celle de l'OS le plus fragile et de plus il existe des logiciels permettant de lire sous un OS les autres partitions en ignorant alors les sécurités (exemple : lecture de fichiers NTFS sans tenir compte des droits).[11]

III. 2.3. Antivirus :

L'antivirus est probablement le premier bloc de protection. Il s'avère nécessaire depuis le développement d'internet, qui est rapidement devenu le principal vecteur de virus, notamment à travers le courrier électronique. Il s'agit d'un logiciel dont le rôle est de détecter et neutraliser des logiciels malveillants communément appelés virus. Les antivirus utilisent principalement deux techniques d'analyse pour détecter les menaces: l'analyse par signatures, destinée à trouver les virus connus et l'analyse heuristique, destinée à trouver les virus inconnus.

- L'analyse par signature consiste à comparer le code d'un fichier à des morceaux de codes caractéristiques de virus connus contenus dans une base de données appelée liste de signatures ; cette liste de signatures doit être mise à jour régulièrement.
- L'analyse heuristique, moins fiable, consiste à rechercher dans un fichier un code suspect pouvant être celui d'un nouveau virus.

III. 2.4. Pare-feu :

- **Un pare-feu (Coupe-*feu*, *garde-barrière*)**, *appelé* **firewall** en anglais, est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Il constitue un des composants matériel ou logiciel de réalisation de la politique de sécurité, qui est la politique de sécurité réseau, celle –ci définissant quels sont les types de communication autorisés sur

le réseau informatique, et aide à empêcher les utilisateurs ou les logiciels malveillants d'accéder à l'ordinateur via un réseau ou internet. Un pare-feu peut également empêcher votre ordinateur d'envoyer des éléments logiciels nuisibles à d'autres ordinateurs. Il évoque donc une porte empêchant les flammes d'Internet d'entrer chez soi et/ou de « *contaminer* » un réseau informatique. Le schéma suivant illustre la façon dont un pare-feu fonctionne.

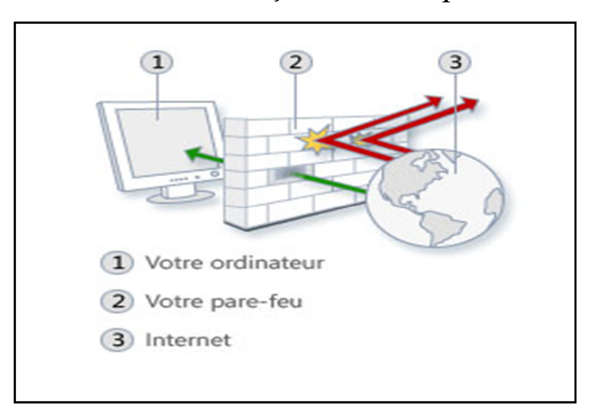


Figure3 : La façon de fonctionnement d'un pare feu

III. 2.5.Authentification :

On considère l'authentification un impportant problème de sécurité. Le système de protction dépend de la capacité à identifier les programmes et les processus en cours d'exécution et cette capacité s'appuie sur la possibilité d'identifier chaque utilisateur du système. Et tellement l'utilisateur s'identifie lui-même, et généralement la procédure d'authentification s'effectue sur une combinaison de trois ensembles d'éléments : **Possession utilisateur**(une clé ou une carte), **Conaissance utilisateur**(un identificateur utilisateur ou un mot de passe) et **attribut utilisateur**(empreinte digitale, configuration de la rétine ou signature), alors l'approche la plus commune pour authentifier l'identité d'un utilisateur est l'utilisation d'un mot de passe.

Quand l'utilisateur s'identifie lui même par le nom d'identification ou le nom de compte, on lui demande un mot de passe. Si le mot de passe fourni par l'utilisateur correspond à

celui qui est stocké dans le système, ce dernier suppose que l'utilisateur est légitime.

L'objectif de mot de passe c'est la protection des objets dans un sysème informatique, par exemple on peut protéger un fichier par l'association d'un mot de passe, et comme on peut utiliser des mots de passe différents pour lire, ajouter et actualiser un fichier.

Certainement qu'il existe des problèmes en rapport avec l'utilisation des mots de passe, parcequ'ils sont facile à employer et à comprendre. Le problème qui se pose avec les mots de passe, c'est la difficulté de les garder secrets.

Les mots de passe peuvent étre compromis parcqu'on les devine, on les expose accidentellement ou on les transfert illégalement d'un utilisateur autorisé à un non autorisé.

Deux façons commune de deviner un mot de passe. L'intrus (humain ou pogramme) peut connaitre l'utisateur ou posséder des informations sur ce dernier. On emploie fréquèment comme mot de passe une information évidente (comme le nom du chat ou de l'épouse). On peut même utiliser la force brute, en essayant toutes lles combinaison possibles de lettres, de chiffres et signe de ponctuation, jusqu'à ce que l'on découvre le mot de passe. Les mots de passe court ne laissent pas suffisament de choix pour éviter d'être découverts par des essais répétés. On donne l'exemple d'un mot de passe qui comporte quatre chiffre décimaux propose seulement 10000 variations. En moyenne, on obtiendrait le mot de passe en essayant 5000 fois. Et si l'on pouvait écrir un programme pour essayer un mot de passe toute les milisecondes, il faudrait à peu prés 5 secondes pour deviner le mot de passe.

Par conséquent, les mots de passe plus longs sont moins susceptible d'étre devinés par énumération et les sytèmes ermettant d'employer dans les mots de passe des majuscules, des miniscules, des chiffres et tous le caractéres de ponctuation rendent la découverte du mot de passe bien plus ardue.

La conclusion c‘est que les utilsateurs doivent en profiter et ne pas employer que des miniscules.

L’échec de la sécurité de mot de passe à cause de son exposition peut provenir de la surveillance éléctronique ou visuelle. Un intrus pourait regarder par dessus l’épaule d’un utilisateur quand il se connecte au système et apprendre facilement le mot de passe. De plus, toute personne ayant accés à un réseau dans lequel se trouve un ordinateur pourrait ajouter un moniteur du réseau lui permettant de voir toutes les données transférées au réseau, y compris les noms d’identification des l’utilisateurs et les mots de passe. L’exposition du mot de passe est un problème serieux s’il est écrit à un endroit oû il peut étre lu ou perdu. C’est pour ça que cretains systèmes imposent à l’utilisateur de séléctionner des mots de passe longs ou difficiles à mémoriser. Mais attention dans le cas extrème, cela peut pousser l’utilisateur à enregistrer le mot de passe, fournissant ainsi une sécurité pire que lorque le système autorise des mots de passe faciles !

La dernière méthode se compromettre un mot de passe est une conséquence de la nature humaine. La plupart des installations informatiques ne permettent pas aux utilisateurs de partager les comptes. Cette règle est quelquefois imposés pour des raisons de comptabilisation, mais souvent pour augmenter la sécurité. Par exemple, si un nom d’identification est partagé par plusieurs utilisateurs et qu’une infraction à la sécurité se produit à partir de ce nom, il est impossible de savoir qui utilisait ce nom d’identification à ce moment là ou même si c’était l’un des utilisateurs autorisés. Avec un seul utilisateur par nom d’identification, on pourrait directement interroger l’utilisateur sur l’utilisation de compte. Quelquefois, les utilisateurs ne respectent pas les règles de partage d’un compte pour aider des amis ou contourner la comptabilisation, et ce comportement peut provoquer que des utilisateurs non autorisés, éventuellement malveillants, accédent à un système.[12]

III. 2.6.Cryptage :

Les gents ont toujours ressenti le besoin de dissimiler des informations, même avant l'apparition des premiers ordinateurs et tellement internet a évolué et est devenu un outil essentiel de communication, ainsi que les réseaux informatiques gagnent en popularité, des inormations (classées) plus confidentielles sont transmises au travers de canaux où l'écoute clandestine et l'interception de messages sont possible. Pour conserver la sécurité de cette information confidentielle, on a besoin de mécanismes permettant à l'utilisateur de protéger les données transfrées à travers le réseau. Alors la cryptographie s'en charge de garantir la sécurité de ces informations.

Par **cryptographie** on désigne l'ensemble des techniques permettant de **chiffrer** des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe **crypter** est parfois utilisé mais on lui préfèrera le verbe *chiffré*. Le cryptage est une méthode courante de protection de l'information, son mécanisme de base fonctionne comme suit :

1) L'information (texte) est cryptée (codée) à partir de sa forme initiale lisible (applée texte en clair) à une forme interne (appelé texte chiffré). Cette forme de texte interne, bien que lisible, n'a aucun sens.
2) Le texte chiffré peut être stocké dans un fichier lisible ou transmis à travers des canaux sans protection.
3) Pour rendre le texte chiffré compréhensible, le récepteur doit éffectuer le décryptage pour obtenir le texte en claire.

Même si une personne non autorisé accède à l'information crypté, l'effort sera inutile sauf si on peut la décoder.

III. 2.7.Détection d'intrusion :

Malgré que l'intrus parvient à franchir les défenses des barrières de protection tel que les pare-feu et les systèmes d'authentification, c'est encore possible de le faire arrêter avant qu'il n'attaque. Les outils de détection d'intrusion qui décèlent tout comportement anormal ou trafic suspect, ont été placés sur

le réseau d'entreprise pour ausculter en permanence le trafic repérer le *hacker* et alerter aussitôt l'administrateur.

On appelle **IDS** (*Intrusion Detection System*) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion. On prend l'exemple de ***Snifer (Ecoute du réseau)*** qui portent l'image d'analyseur de réseau et permet d'intercepter certaines informations qui transitent sur un réseau, encore il est outil de détection d'intrusion qui s'installe à un point stratégique du réseau. Il analyse en permanence le trafic à la recherche d'une signature connue de piratage dans les trames. Ce système ne repère que les attaques qui figurent déjà dans leur base de signatures.

III. 2.8. Sauvegarde de données et documents:

La sauvegarde régulière des données et de la documentation qui permet de les utiliser est bien sûr un élément indispensable de la sécurité du système d'information, par ce qui suit on mentionne quelques règles de bon sens qui sont :

☞ Définition de type de données à sauvegarder, selon quelle périodicité, pour quelle durée est une obligation légales pour certaines données – Revoir périodiquement le périmètre de sauvegarde.

☞ Dupliquer les sauvegardes - Répartir les informations confidentielles sur plusieurs supports.

☞ Sécurisation des lieux de sauvegardes, conservation des supports mensuels et annuels en dehors de l'entreprise.

☞ les supports de sauvegarde doivent être stockés de façon à être disponibles après un sinistre tel qu'incendie ou inondation: armoire ignifugée étanches ou site externe.[13]

Conclusion :

En conclusion, La sécurité des systèmes d'information est une tâche à prendre en compte par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent et assurent la gouvernance de son système d'information. Au fur et à mesure que les systèmes informatique sont devenus plus sophistiqués et perspicaces dans leur application, le besoin de protéger leur intégrité a également augmenté, et le rôle de la protection dans un système informatique est de fournir un mécanisme pour appliquer les politiques gouvernant l'usage des ressources, et donc la sécurité doit prendre en compte le système informatique et l'environnement dans lequel le système est utilisé. Pour un système d'information donné, la menace n'est pas unique mais le plus souvent composite du fait de la diversité des systèmes et des informations gérées.

Au final, la sécurité de l'information reste un point important des organisations, les données stockées dans le système informatique doivent être protégés des accès non autorisés, de la destruction ou d'une altération malveillante et de l'introduction accidentelle d'incohérence. Il est plus facile de protéger contre la perte accidentelle de la cohérence de données que contre les accès malveillants aux données. La protection absolue de l'information stockée dans un système informatique contre l'abus malveillant n'est pas possible, mais le cout pour l'auteur du crime peut être rendu suffisamment élevé pour décourager la plupart, sinon la totalité, des tentatives d'accéder à cette information sans l'autorisation adéquate.

Références bibliographie

1- [Document approuvé et signé par le sous-ministre, V1.0, 10 mai 2015], Politique de sécurité de l'information.
2- https://fr.wikipedia.org/wiki/Portail:S%C3%A9curit%C3%A9_informatique, Portail sécurité informatique.
3 - LESCOP Yves [V1.6], La sécurité informatique

4 - [Solange Ghernaouti], Sécurité informatique et réseau, [4e édition]
5 - Un enjeu majeur pour la France, Sécurité des systèmes d'information
6 - [Solange Ghernaouti], Sécurité informatique et réseau, 4e édition
7 - Un enjeu majeur pour la France, Sécurité des systèmes d'information
8 - [Robert Longeon Et Jean-Luc Archimbaud], Guide de la sécurité des systèmes d'information.
9 - Un enjeu majeur pour la France, Sécurité des systèmes d'information
10 - [Joseph ILLAND, Novembre 2006] : Politique de sécurité des systèmes d'information.
11 - LESCOP Yves [V1.6], La sécurité informatique
12 - [Abraham Silberschatz et Peter b Galvin], Principes des systèmes d'exploitation, 4e édition
13- [Laurent Bloch, Christophe Wolfhugel], Sécurité informatique, Principes et méthodes, 3e édition

دراسة تقابلية انجليزية/عربية لمصطلحات عالم الاختراق وعلاقتها بالأمن المعلوماتي

ليلى يمينة موساوي

مركز البحث العلمي والتقني لتطوير اللغة العربية جامعة تلمسان.

ملخص: عموما كلمة "هاكرHacker" توصف المختص المتمكن من مهارات في مجال الحاسوب وأمن المعلوماتية. وأطلقت كلمة هاكر أساسا على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهارتهم. إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب أن يكونوا فيه. والقيام بهذا عملية اختيارية يمتحن فيها المبرمج قدراته دون أن يعرف باسمه الحقيقي أو أن يعلن عن نفسه. ولكن بعضهم استغلها بصورة إجرامية تخريبية لمسح المعلومات والبعض الآخر استغلها تجاريا لأغراض التجسس والبعض لسرقة الأموال. في هذا الورقة البحثية سنقوم بدراسة تقابلية بين الانجليزية والعربية لبعض المصطلحات التي لها علاقة بعالم الاختراق المعلوماتي لنبين المفاهيم الجديدة للمصطلحات التقنية الحديثة التي دخلت في قاموس معجم اللغة العربية.

Abstract :

Generally the word "Hacker" described competent mastery of skills in the field of computer and information security. And it launched the word hacker essentially a set of clever programmers who unite the different systems and try to storm it, not necessarily to be in the intention to commit a crime, or even a misdemeanor, but their success in penetration is considered a success for their abilities and skills. However, the law considered them outsiders managed to enter the default venue should not be in it. And to do this optional process in

which the programmer tested his abilities without knowing his real name or to announce himself. But some of them are exploited by criminal sabotage to clear information, others are commercially exploited for the purposes of espionage and to steal some money. In this paper we will make a contrastive study between English and Arabic to some of the terms that are related to the world of penetration informational to show new concepts of modern technical terms that have entered into Dictionary Lexicon Arabic.

مقدمة: من أهم مفردات الانجاز العلمي والحضاري هو التعريف بالمفاهيم والمصطلحات التي تحمل الفهم السليم للظواهر والأحداث وقد دفع بروز دور ثورة المعلومات والاتصال إلى ثورة معرفية جديدة لا تتعلق فقط بما أضافته إلى الحياة المعاصرة بل أيضا إلى الدفع إلى إعادة النظر في مفاهيمنا القديمة التي تتعلق بنظر الإنسان إلى الكون والأشياء والى ذاته، وأدت ثورة الإعلام والاتصال إلى حدوث طفرة هائلة في المصطلحات ذات الطبيعة الفنية تارة ثم إلى تحولها إلى مفاهيم عامة تهم أيضا مستخدمي تكنولوجيا الاتصال والمعلومات وذلك بعد حدوث دمج متصاعد بين الطابع التقني والحياة المدنية التي تهم كافة البشر لما لها من علاقة بالتقدم الإنساني، وكان من أهم تحديات تلك الثورة وتلك الخدمات هو كيفية الحفاظ على الأمن والخصوصية في ظل تحديات كبرى تشكل تهديد لأمن الانترنيت والبيانات الشخصية، ويمثل أمن المعلومات مفهوم واسع وأيضا يدخل في اهتمام كافة القطاعات الحكومية والخاصة والمجتمع المدني.

وفي إطار احتمالية التعرض للأخطار الالكترونية وتهديد مصالح الحياة لكافة الناس وهو ما يستلزم أهمية دور الوعي في منظومة الحماية ومن أهم مفردات ذلك تبسيط المصطلحات وتسهيل فهمها للمستخدمين من أجل دعم الوعي والحماية ضد الأخطار والتهديدات بالإضافة إلى نشر معرفة موحدة للمصطلحات التكنولوجية وخاصة مع بعض المشكلات في تعريب بعضها. فما هي معايير نقل مصطلحات

الأمن المعلوماتي إلى العربية من مصدرها الانجليزي؟ وهل هي ترجمة للمفهوم أم تعريبا للمصطلح؟ وهل يجب ترجمة كل ما هو تقني إلى اللغة العربية؟

1- **المصطلح التقني ومشكلات الترجمة التقنية:** في عصر المعرفة وتشعب العلوم والانفتاح الحرّ وتلاشي الحدود والحواجز بين الأمم ازدادت الحاجة الى الترجمة العلمية التي تتطلب ترجمة وتعريب المصطلحات العلمية والتقنية المتميزة بنشأتها في بيئة غربية غير عربية. ولا شك أن نقل المصطلح من البيئة اللغوية والثقافية التي نشأ فيها يجعله غريبا في اللغة المنقول اليها لاختلاف الأنظمة اللغوية وأبنية الكلمات بين اللغتين، واذا كان يصعب على المبتكر وضع مصطلح يعبر به عن مفهوم ما بلغته ومن نسيجه فكيف ي حال من ينقله من لغته الأصلية التي غالبا ما تكون أعجمية الى العربية. علما أنه يدخل ساحة المعرفة في العالم ما يزيد 18000 مصطلح جديد سنويا، أي بمعدل 50 مصطلحا كل يوم، وأما المقابلات العربية التي توضع فلا يتجاوز عددها سنويا 2500 مصطلح تقريبا[1].

1-1- **تعريف المصطلح التقني:** هو كلمة أو عبارة لها معنى خاص في مجالات العلوم والتقنيات الهامة المعترف بها كالميكانيك، والالكترونيات والمعلوماتية وغيرها. وليس من السهل تحديد مفهومها بخاصة اذا ما ارتبط بمجالات بلغت أقصى درجات التقدم التكنلوجي، ولعل هذه الصعوبة تشكل واحدة من بين أسباب اقتصار استعمال المصطلح التقني على اختصاصيين ومهندسين.

ويعرف علي القاسمي المصطلحات التقنية بأنها مجموعة من الرموز اللغوية التي تدل على مفاهيم أو أشياء تتعلق بفرع من فروع العلم والتكنولوجيا. ويضيف الى هذا الحد معيارين تعرف من خلالهما جودة المصطلح. يتمثل الأول في وضع مصطلح مستقل وأما الثاني فيكمن في تسميته المفهوم الواحد بمصطلح واحد لا أكثر. والحقيقة أنه قلما نجد مصطلحا علميا أو تقنيا يتوفر فيه هذان الشرطان. وعلى عكس الكلمات التي تنتمي إلى اللغة العامة، تميز المصطلح التقني لغة

خاصة وكتابة معينة تتجلى في الوثائق المعروفة بتقنيتها كالمراجع، ونشرات الصيانة، ووصف التجهيزات أو طرائق الاستعمال[2].

1-2- مفهوم اللغة التقنية: قد لا يفرق الكثير منا بين لغة التخصص واللغة التقنية لكونهما تشتركان في الدقة، والاختزال، والوضوح، والبساطة، حيث أن الأولى أشمل من الثانية وتجمع بين العديد من التخصصات تستخدم لغة خاصة بالمعرفة التي تستوعبها كلغة الاقتصاد، ولغة القانون، ولغة الإدارة، ولغة الهندسة ولغة الرياضيات، ولغة علوم الطبيعة والحياة، بينما اللغة التقنية كالهندسة المدنية والميكانيكية والالكترونيات والإعلام الآلي وغيرها.

يعرف ف.لازار F.Lazar اللغات التقنية بأنها لغات تهدف إلى تنقية معجمها وتركيبها ودلالتها ليتم التوصل إلى معرفة مؤديات تخلو من أي لبس. يركز هذا التعريف على ضرورة وضوح الدلالة والمعنى واللفظ، في اللغة التقنية للتوصل إلى المضامين العلمية المقصودة[3].

وعند مقارنة نصوص اللغة العامة بالنصوص التقنية، نجد أن الاختلاف الجوهري بينهما يكمن في المصطلحات. فاللغة التقنية تضم عدد كبير من المصطلحات غير موجودة في اللغة العامة، أو ربما نجدها ولكن بمعنى مختلف تماما، على سبيل المثال نأخذ مصطلح **Souris** الذي ترجم إلى العربية **بالفأرة** فهو موجود في كلتا اللغتين إلا انه يحمل معنى حيوان في اللغة العامة أما في اللغة المتخصصة فمعناه آلة تابعة لجهاز. لذا فتعدد الألفاظ الدالة على مفهوم واحد مسموح به في اللغة العامة ولا يسمح به في لغة التخصص تفاديا للبس.

يتضح مما تقدم الصعوبة التي يواجهها المترجم عند تعامله مع اللغة التقنية لاسيما عندما يتعلق الأمر بمجالات يجهلها، ففضلا عن المصطلحات التقنية الغاضة يجد المترجم نفسه أمام مفاهيم مجردة وتفكير منطقي معقد.

1-3- المصطلح في اللغة التقنية: يمكن تصنيف المصطلحات حسب عدة معايير نحصرها في الشكل، والمعنى، والوظيفة[4].

1- **3-1- الشكل:** قد تكون المصطلحات بسيطة أو معقدة، حسب عدد المورفيمات، نحو:(Radio, Radioscopie) "صورة مشعاعية، تنظير شعاعي" (lumière, liminescence) "ضوء، إضاءة".

- قد تتشكل المصطلحات المعقدة من كلمتين فأكثر، مثل:(mémoire vive) "ذاكرة حية".

(Système de gestion de base de données) "نظام تسيير المعطيات". تكثر في اللغة التقنية مصطلحات تبدو بسيطة من الوهلة الأولى ولكن أصلها مركب كالمختصرات.

1-3-2-المختصرات: نظام إملائي اعتباطي مختصر، وضع للرسم والنطق. أو رمز اختصاري (Abréviation) وخصّه المجمع المصري بالاختصار الكتابي. فهو نظام كتابة سريعة، أو نطق تعتمد الرموز بدل الكلمات أو الجمل. يكثر توظيفه اليوم كوسيلة ثقافية سريعة في مجال الصناعة وفي المعاملات التجارية والإعلانات[5].

وتلفظ الاختصارات بعدة طرق على النحو الآتي:

* قراءة المختصر على أساس أنه كلمة واحدة، نحو: UNESCO يونسكو.

* قراءة كل حرف على حدة، نحو (PC)، اختصار لـــــ"حاسوب محمول".

* قراءة المختصر باستخدام الطريقتين الأولى والثانية معا، مثل: (CD-Rom)[6].

ولغة علم الحاسوب، كغيرها من اللغات العلمية والتقنية، تستخدم الرموز والمختصرات بكثرة لتسمية بعض من مفاهيمها والغاية من وراء هذا الاستخدام هي اختصار المصطلحات التي تتكون من مجموعة من الكلمات، وتيسير التواصل بين مهندسي الإعلام الآلي في العالم.

1-3-3- المعنى: تقترح ماريا تيرزا كابري تصنيف المصطلحات حسب نوع المفاهيم التي تنتمي إليها، وهي أنواع:

- أشياء وكائنات (سيارة، طائرة).
- صفات (مرئية، سمعية، ملموسة، مادية، مشتركة، وغيرها).
- أنظمة أو عمليات (تلحيم، فصل، طوي).

1-3-4- الوظيفة النحوية: يمكن تصنيف المصطلحات حسب وظيفتها النحوية في الخطاب، قد تكون صفة، فعل، فاعل...الخ[7].

2- تقنيات الترجمة:

- الترجمة العامة:

تقترن طرق الترجمة بالنصوص بصفة عامة، وقد اقترح بيتر نيومارك طريقتين لترجمة النصوص التقنية، وهما الترجمة التواصلية (Communicative Translation) والترجمة الدلالية (Semantic Translation)[8].

- الترجمة التواصلية: هي طريقة تقوم على نقل المعنى السياقي الدقيق الأصلي بحيث يتقبل القارئ المستقبل الرسالة ويفهمها بيسر شكلا ومضمونا.

- الترجمة الدلالية: هي طريقة تعتمد على إعادة إنتاج المعنى السياقي الدقيق بحذافيره في اللغة الهدف مراعية في ذلك مقاصد المؤلف الأصلي والبنية الصرفية للغة الهدف.

أما إجراءات الترجمة فتستعمل للجمل والوحدات اللغوية الأصغر، وأن أول ما يتبادر إلى أذهاننا بمجرد الحديث عن تقنيات الترجمة هو أول ظهور للأسلوبية المقارنة (Stylistique Comparée) من خلال كتاب "فيني" و"داربلني (J.P Vinay & Darbelnet) المعنون بــ: "دراسة أسلوبية مقارنة بين اللغتين الفرنسية والانجليزية"، اقترح فيها المؤلفان سبع مناهج تقنية للترجمة بين اللغتين الفرنسية والانجليزية تنقسم إلى ترجمة مباشرة (Traduction Directe) تضم ثلاث تقنيات وترجمة غير مباشرة (Traduction Oblique) تشتمل على أربع منه[9].

2-1- الترجمة المباشرة(La Traduction Directe):

تعتمد هذه الطريقة في الترجمة بين لغتين لا تختلفان كثيرا في المبنى والمعنى أي عندما يكون تركيب الجملة أو المفهوم واحدا[10].

2-1- 1- الاقتراض: (L'emprunt)

عندما يجد الكاتب الذكي نفسه محاصرا بين أقسية الاشتقاق والابتكار وحرمة الاختراع والتجديد، يلجأ إلى الاقتراض من أي لغة كانت ليسد حاجته الذهنية في التعبير عندما تضيق به ألفاظ اللغة عن تأدية بعض الصور الفنية، عندما يلجأ إلى الاقتراض من أي لغة أخرى، والاقتراض هنا يشمل هنا استعارة ألفاظ إما أن تكون فارسية أو عثمانية أو يلجأ إلى الترجمة من اللغات الأوروبية كالانجليزية أو الفرنسية، وهو ما يسمى بالتعريب خصوصا ما عناه الكتاب في بداية القرن العشرين حتى أواخره خصوصا في كثير من المصطلحات العلمية[11] وهذا ما تنبه إليه الجواليقي[12]. فاللغات تقترض بعضها من بعض ويقتصر الاقتراض عادة على الألفاظ والكلمات ولا تكاد تتعداها، أما الاقتراض الذي تدعو الحاجة إليه فقد عرفه القدماء، كما عرفه المحدثون، فقد اقترض العرب من الفرس واليونان ألفاظا للتعبير عن أشياء ليست في بلاد العرب، وعمد القدماء إلى بعض الألفاظ فحوروا من بنيتها وجعلوها على نسج الكلمات العربية...[13].

2-1-2- النسخ : هي نوع خاص من الاقتراض، يتم من خلاله اقتراض صيغة تركيبية موجودة في اللغة الأصل وذلك بترجمة العناصر المكونة لهذا التركيب. مثل:"La première dame"، في الفرنسية تترجم "بالسيدة الأولى" في العربية.

2-1-3- الترجمة الحرفية (La traduction Littéral): هي استبدال كلمة بكلمة أخرى مقابلة لها في لغة ثانية. فيتحصل المترجم على نص سليم في اللغة الهدف مكتوب بلغة شائعة وما عليه سوى تحمل التبعية اللغوية. وليست الترجمة الحرفية دائما مستحبة، إذ يقول محمد الديداوي: "إن الترجمة الحرفية تل ناقصة

وقد تكون سببا في تخريب اللغة وإفسادها، وقد تساعد الترجمة الحرفية على الاحتفاظ بـــــ"النكهة الأصلية"[14].

2-2- الترجمة غير المباشرة: La traduction oblique

2-2-1 الإبدال: La transposition : هي تقنية تقوم على تغيير عنصر من أقسام الكلام أو ترتيبه بعنصر آخر مع الحفاظ على المعنى الإجمالي للرسالة. ويستخدم هذا الإجراء لأغراض أسلوبية تتطلبها اللغة الهدف مثل: dés son lever تنقل إلى اللغة الانجليزية على النحو الآتي: As soon as he gets up، لأن اللغة الانجليزية لا تمتلك إلا حالة واحدة لترجمة هذه الجملة الفرنسية. فيكون هنا الإبدال إجباريا. أما في المثال الآتي after he comes back، تترجم إلى العربية بـــ:"عندما يرجع"، أو "عندما يعود"، "عند رجوعه". فالإبدال هنا اختياري لأن اللغة العربية لديها إمكانيات للتغيير.

2-2-2- التعديل La modulation: هي تقنية تعتمد على تغيير وجهة النظر أو في درجة الوضوح عند نقل الرسالة الأصلية إلى اللغة الهدف، كاستخدام اسم الجزء للتعبير عن اسم الكل، أو المجرّد للتعبير عن الملموس وقد يكون التعديل اختياريا أو ضروريا.

2-2-3 التكييف L'adaptation : تقنية تستخدم لنقل موقف معين إما غير موجود في اللغة المترجم إليها وإما منافيا لعادات وتقاليد تلك اللغة. يقول الفرنسي un froid de canard، في حين يقول العربي "البرد قارص"[15].

- ترجمة المصطلحات: أشار محمد رشاد الحمزاوي عند حدثه عن تقنيات الترجمة –يقصد ترجمة المصطلحات- اعترافا منه وتقديرا بأن هذا النوع من الترجمة الذي يمثل جزءا أساسيا من ترجمة النص، يتحتم أن تكون له قواعده وضوابطه–أشار إلى عدد من المعايير استنادا إلى المدرسة الكندية وبخاصة فيناي وداربلني ولخص هذه الإجراءات فيما يلي[16]:

أ- الترجمة المباشرة: وهي تعني النقل من اللغة الأصل إلى اللغة الهدف سواء لتوافق بنيوي أو اصطلاحي، بل أن ذلك التوافق معدوم مع العربية وهو ناتج غالبا عن ثغرات وفراغات توجد في اللغة المترجم إليها.

- الاستعارة (التعريب): وهي عبارة عن تحويل كلمة في نص اللغة المصدر إلى نص اللغة الهدف، وتستخدم في حالة وجود مفاهيم جديدة لا يمكن للغة المترجم إليها أن تعبر عنها.

- النسخ: وهو نوع من الاستعارة الخاصة وذلك بأن نأخذ العبارة من اللغة المترجم عنها وتترجم ترجمة مباشرة تستوجب إدخال استعمال جديد يبدو غريبا. نحو "الدرجة الصفر" « Zéro degré ».

- التضخيم: بالمعنى الفزيائي وهو الحال الذي تستعمل فيه اللغة المترجم إليها كلمات أكثر من كلمات اللغة المترجم منها[17].

- التحشية: وهي تشبه التضخيم مع زيادة في الألفاظ.

ب- الترجمة الجانبية: وهي تحتوي على:

- التكافؤ: وهو التعبير عن مصطلح اللغة الأصل مع اعتماد تعبير مختلف.

- المؤالفة: وهي اعتماد مقابل خاص من لغة ما لتأدية معنى خاص بلغة أخرى.

- التحوير: وهو يفيد التجديد والقطيعة بين المفاهيم القديمة والحديثة ليستمد مصطلحاته من المعاجم المقررة بل هو من وضع المترجمين لتأدية مفاهيم جديدة. وقد التقى مع نيومارك في بعض هذه الأنواع كالنسخ (التحويل)، الاستعارة (التطبيع)، التضخيم (المقابل الوصفي)...الخ[18].

3- دراسة تطبيقية لعينة من مصطلحات عالم الهاكر؛ دراسة تقابلية انجليزية/عربية:

3-1- ما هو الاختراق؟ هاكر، اختراق، قرصنة...كلمات باتت تخيف الناس خصوصا مستخدمي الإنترنيت، الجميع يريد الحماية ويريدون من ينقذهم من هذا الكابوس القابع تحت مسمى القرصنة. فالهاكرز هو عالم كبير وبدايته كانت قبل الانترنيت وقبل الكمبيوتر نفسه، وقد انتشر هذا المصطلح انتشارا رهيبا في الآونة الأخيرة وأصبح يشير بصفة أساسية إلى الأفراد اللذين يلجئون بطريقة غير شرعية إلى اختراق أنظمة الحاسب بهدف سرقة أو تخريب أو إفساد البيانات الموجودة بها. وفي حالة قيام المخترق بتخريب أو حذف أي من البيانات الموجودة يسمى (كراكر)، لأن الهاكر يقوم عادة بسرقة ما خفي من البرامج والملفات ولا يقوم بالتخريب أو التدمير[19].

3-2- الدوافع الرئيسية للاختراق هي: لم تنتشر هذه الظاهرة لمجرد العبث وان كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها إلى عالم الوجود والدوافع الرئيسية للاختراق نوجزها في ثلاث نقاط هي:

- الدافع السياسي والعسكري: مما لا شك فيه أن التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع المعلوماتي والتجسسي بين الدولتين العظمتين آنذاك على أشده. ومع بروز مناطق جديدة للصراع في وتغير الطبيعية المعلوماتية للأنظمة والدول، أصبح الاعتماد كليا على الحاسوب الآلي. وعن طريقه أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.

- الدافع التجاري: من المعروف أن الشركات التجارية الكبرى تعيش هي أيضا فيما بينها حربا مشتعلة (الكوكا كولا والبيبسي على سبيل المثال) وقد بينت الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجري عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم.

– الدافع الفردي: لمجرد أن يثبت الشخص لنفسه أو لغيره قدرته على تطوير برامج تستطيع الاختراق أو التجسس أو التخريب. وهذا غالبا ينتشر بين صغار السن أو المبتدئين.

– الانتقام من أفراد، أو شركات أو دول، مثلا نجد عديدا من المطورين يحاولون النيل من شركة ميكروسوفت لاستحواذها وسيطرتها على الأسواق البرمجية.

– للابتزاز، فهناك من الخبثاء من يقوم بسرقة معلومات مهمة لشركة، ثم يقوم بمساومة الشركة على تلك المعلومات[20].

3–3– التحليل والترجمة: **Hacker/Cracker/Attacker**

مخترق/ مخرب/مهاجم

الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف... وحينما نتكلم عن الاختراق بشكل عام فنقصد بذلك قدرة المخترق على الدخول إلى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول إلى جهاز آخر فهو "**مخترق**" «**Hacker**» أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو "**مخرب**" «**Cracker**». وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين عنوة ودون رغبة منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو بنفسياتهم عند سحب ملفات شخصية كالصور والفيديوهات وغيرها[21].

* الترجمة المقترحة:

– ترجم المصطلح ترجمة مباشرة حرفية إذ يوجد تكافؤ شكلي بين المصطلحين، أما في اللغة العربية فنجد له عدة معاني دلالية ومعجمية منها: التخريب، القرصنة، التطفل، السرقة، التجسس، التسلل، العبث، اقتحام، هجوم تدمير، تصديع [22]...الخ.

– أما التقنية الثانية المستعملة هي تعريب أو اقتراض المصطلح مباشرة: "**هاكر**" و"**كراكر**" لأن هناك من يفضل المصطلح الانجليزي كما هو لأنه أصبح أكثر تداولا بالرغم من وجود المقابل العربي.

Physhing

الاصطياد الالكتروني

تعني رسائل الاصطياد أو التصيّد الالكتروني: سرقة البيانات الشخصية السرية والحساسة عن طريق رسائل البريد الالكتروني لغرض انتحال الشخصية، وذلك عن طريق انتحال شخصية أحد المصارف، أو منظمة معينة وإيهام الضحية بجدية الطلب وأهميته[23]. وهي رسائل تبدو بالشكل والعنوان البريدي أنها مرسلة من منظمة حقيقية (وغالبا ما تكون المنظمة بنكا)[24]. سمي هذا النوع من الرسائل رسائل الاصطياد الالكتروني أو رسائل الاصطياد الخادعة Physhing « Scam/Spam » لأن مرسليها يستخدمون رسالة البريد الالكتروني لطعما لاصطياد الأرقام السرية وغيرها من البيانات الشخصية الحساسة الأخرى من بحر مستخدمي الشبكة العالمية. كان أوائل مخترقي الشبكة العالمية (Hackers) عادة ما يستبدلون الحرفين (Ph) بالحرف (f) لإنشاء كلمات جديدة في مجتمعهم، أي مجتمع قراصنة الشبكة العالمية، كون النطق هو نفسه، ولكن الكتابة تختلف. نشأت كلمة (Physhing) في تسعينات القرن العشرين من الكلمة (Fishing) التي تعني اصطياد الأسماك[25].

- الترجمة المقترحة: ترجم المصطلح حرفيا إذ يحمل نفس المعنى الدلالي في الانجليزية، "To Fish" تعني "يصطاد" مع استعمال تقنية التضخيم في زيادة لفظ "الكتروني" لتحديد المعنى الذي يفيده مصطلح "الاصطياد" وهذا ما يسمى بالتطور الدلالي للمصطلح فمن صيد السمك بالطعم في المياه إلى اصطياد كلمة المرور أو أرقام سرية للمستخدم في الشبكة العنكبوتية.

Malware Attack/Malicious codes

البرامج الخبيثة

المصطلح مركب من كلمتين Mal وWare

Mal: تعني شيء خبيث وضار ومفسد

Ware: اسم (في الكلمات المركبة) كل ما هو مصنوع من نوع خاص من المواد، أو ملائم لاستخدام خاص.

التعريف الاصطلاحي: البرامج الخبيثة هي أي برنامج يكون كل مهامه أو أحدهما عمل خبيث من تجسس أو تخريب، أو استنزاف للموارد (الوقت، المعالج الذاكرة، وحدة التخزين، سعة النقل الشبكي وغيرها...)[26]. تسمح هذه البرامج الخبيثة للصيادين بمراقبة جميع العمليات المنفذة من خلال متصفح الشبكة العالمية من قبل المستخدم (الضحية)[27].

تحليل المصطلح والترجمة: عند المقابلة بين المصطلحين الانجليزي والعربي نجد تقابلا شكليا بينهما لأن الأول كلمة مفردة مركبة من كلمتين اثنين " Mal "و" Ware "و"Mal" هي اختصار لكلمة "Malicious"، والثاني جاء في كلمتين اثنتين في صيغة الجمع "البرامج الخبيثة". بالإضافة إلى أن المقابل الانجليزي المعروف لــ "برنامج" هو «program» وهو مصطلح يستخدم في علم مجال علم الحاسوب كما يستخدم في مجالات أخرى، فكانت المؤالفة هي التقنية المستخدمة.

Viruses

الفيروسات

أصل الكلمة: تشير الكلمة اللاتنية Virus إلى السم القاتل وغيره من المواد الضارة، أما معناها "العامل المسبب للأمراض المعدية". ومصطلح viral يستخدم أيضا للدلالة على الجسم الفيروسي المعدي الوحيد ومجموعها Virion[28].

يعرف الفيروس في علم البيولوجيا على أنه جزئية صغيرة من مادة حية غير قادرة على التكاثر ذاتيا ولكنها تمتلك مادة وراثية كافية لتمكنها من الدخول إلى

خلية حية وتغيير العمليات الفعالة في الخلية بحيث تقوم تلك الخلية بإنتاج جزئيات جديدة م ذلك الفيروس والتي تستطيع بدورها مهاجمة خلايا جديدة.

وبشكل مشابه، يعرف الفيروس في علم الكمبيوتر على أنه برنامج صغير أو جزء من برنامج يربط نفسه ببرنامج آخر ولكنه يغير عمل ذلك البرنامج لكي يتمكن الفيروس من التكاثر عن طريقه، وله أهداف تدميرية تهدف إلى إحداث أضرار جسيمة بنظام الحاسوب سواء بالبرنامج أو المكونات[29]. وعندما يدخل إلى الكمبيوتر يعمل نفس التأثيرات و نفس الأفعال، وله نفس قدرة التكاثر وربط نفسه بالبرامج حتى يسبب دمار الكمبيوتر دمارا شاملا[30].

تحليل المصطلح والترجمة: أخد مصطلح Virus في علم الأحياء نفس المنحنى الدلالي لمصطلح "فيروس" في علم الحاسوب، إذ ترجم حرفيا من اللغة الأصل وهي اللاتينية. كما نلاحظ استعمال نفس الحقل المعجمي والدلالي للمصطلح في كلا الاستعمالين أي العضوي والالكتروني وكأن الحاسوب هو جهاز عضوي نحو: خبيث، مضر، قاتل، سرعة التكاثر، مصاب، التعطيل عن العمل، دمار الأجهزة التطفل، الانتقال بالعدوى....

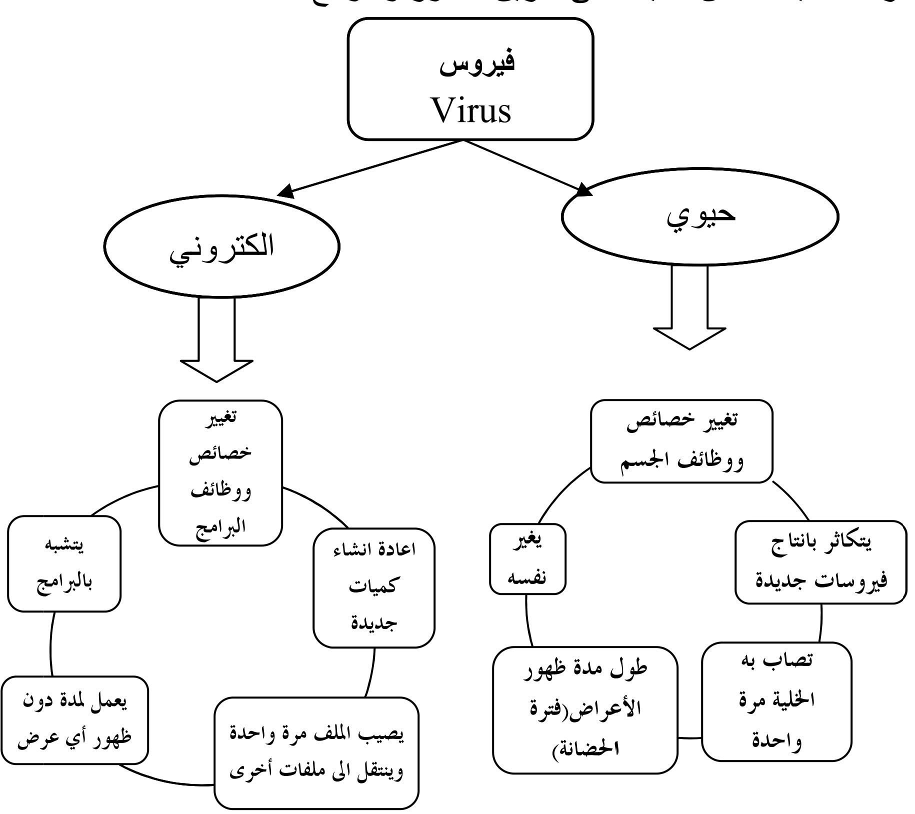
Trojan Horse

حصان طروادة

سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها وهكذا تكون آلية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج دون أن يعلم المستخدم[31]. وذلك لتشابه عمله مع أسطورة حصان طروادة الخشبي الذي اختبأ به عدد من الجنود اليونانيين وكانوا سببا في فتح مدينة طروادة. وهي شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالبا ما تتركز على إضعاف قوى الدفاع لدى الضحية واختراق جهازه وسرقة بياناته[32].

تحليل المصطلح والترجمة: ترجم المصطلح حرفيا وذلك لوجود المقابل اللفظي فكلمة « Trojan » تقابلها "طروادة" وكلمة "horse" تقابلها كلمة "حصان". تطور المصطلح دلاليا فحولت أسطورة بكاملها إلى مصطلح اتخذ مفهوم آخر لأنه استعمل في مجال علم الحاسوب، فالذي أطلق هذا الاسم على هذا الفيروس وكأنه أراد أن يخرجه من عالم القصص والأساطير التي كانت حبيسة الكتب إلى عالم التكنولوجيا المعقد، إذ انتقلت المفردة من معناها الحسي الملموس الى معنى مجرد. ومن هذه الأسطورة استنبط المصطلح للدلالة على ما هو ظاهره نافع مفيد وباطنه ضرر أكيد.

لأن كل المعاني في طورها الأول كانت حسية ملموسة، وبتقدم الحياة والفكر من جهة وقلة المفردات من جهة ثانية، وجد الإنسان نفسه مضطرا إلى لاستعمال مفردات قديمة لمعان جديدة على طريق التجوز والتوسع[33].



خاتمة بأهم النتائج: لقد استهدف البحث استجلاء المصطلحات التقنية بمفهومها الحديث، والتي ظهرت مجددا على الساحة العربية، مع رصد تطورها الدلالي والاحتكاك بالمفاهيم الجديدة لها؛ لأن أهمية البحث اللغوي تتأتى عند تحديد معاني هذه المفاهيم ودلالاتها، لأن دخول مصطلحات جديدة ليس هو المشكلة بقدر ما تكمن المشكلة في المفاهيم التي تعبّر عنها، فالمفهوم كلمة لها دلالتها اللغوية ومعرفة هذه الدلالة هي السبيل الأول لفهم المفهوم، وقد أوصلني هذا المنطق إلى تحديدات واضحة لمفاهيم عدّة.

إن مصطلحات الأمن المعلوماتي بما فيها مصطلحات الاختراق تعبر عن مفاهيم دقيقة لا يستطيع عالم المهندس في علم الحاسوب أو غيره من المهتمين به الاستغناء عنها. ولعل دلالتها محددة بنسبة كبيرة في اللغة الانجليزية (الأصل) باعتبارها منشأ هذا العلم على عكس اللغة العربية، فأثار اهتمامنا مدى توافق هذه الدلالة مع معنى المصطلحات العربية المكافئة لها وحاولنا تحديده في هذا البحث.

ولقد خلص البحث إلى جملة من النتائج يمكن توضيحها في ما يلي:

- يلاحظ أن المصطلحات الأجنبية في غالبيتها ألفاظ مفردة، موجزة سهلة التداول، ومعظمها ذو أصول لاتينية ويونانية، ويعتمد تركيبها بشكل كبير على السوابق اللواحق، أما الترجمات العربية فهي غالبا مصطلحات مركبة. مثل: Malware وهي كلمة مركبة من كلمتين اثنين "Mal "و"Ware "و"Mal" هي اختصار لكلمة "Malicious" يقابله "برامج خبيثة"، وPhyshing Scam/Spam يقابله رسائل الاصطياد الالكتروني أو رسائل الاصطياد الخادعة.

- تطور دلالي في معظم المصطلحات وذلك لارتباطها بمفاهيم مختلفة كارتباط الفيروس بأسطورة "حصان طروادة"، وبأسماء حيوانات كفيروس "الدودة" worm

و"العناكب" spiders، والأرنب "Rabbit" وهذا ما نجده بكثرة في أسماء الفيروسات لكونها برامج خبيثة.

– يميز الترجمات العربية لمصطلحات علم الحاسوب الترادف بين الترجمة والتعريب والاقتراض. ويلفت انتباهنا إلى أن المصطلحات المعربة عرضة للتغيير على مستوى المعنى والشكل خلال تداولها شفهيا وهي أكثر شيوعا على حساب المصطلح العربي رغم سهولته ويسر تداوله كمصطلح "الهاكر". إلا أن استخدام اللغة العربية أكثر من الألفاظ المقترضة في مجال كعلم الحاسوب، لا محدود من حيث التطوّر، خير دليل على قدرتها على مسايرة التطور وإثراء معجمها كمصطلح "فيروس".

وختاما، إن الترجمة والتعريب صنوان متكاملان. فبالترجمة يكون الاطّلاع على معارف الغير وفي سرعتها تعجيل بالفائدة، وبعد الهضم الكامل لما تُرجم والاستفادة منه يتيسّر التعريب، وعند التعريب يكون الإبداع الحقيقي الذي يفضي إلى الرقيّ. وقبل الترجمة والتعريب تلزم متابعة ما يستجد وتتبّع ما يتطور في أصله ابتداءً. إن هذه العملية الثلاثية متلازمة أبدا ولا يجوز أن يختلّ ركن من أركانها. ومن المتّفق عليه أن إيجاد المصطلح يكون إما بالترجمة أو بالاختراع وغالبا ما تسبق هذا تلك. لذا، فإن المترجم، مهما كان نوعه، هو على العموم أول من يصطدم بالمصطلح ويتعامل معه سلباً أو إيجابًا وله دور مؤثّر في هذا الاتجاه أو ذاك، حسب مستواه وما يُتاح له.

المصادر والمراجع:

- حمد عبد الرحمان حمد، عوامل التطور اللغوي؛ دراسة في نحو وتطور الثورة اللغوية، دار الأندلس للطباعة والنشر بيروت لبنان، ط1، 1983.

- خالد بن سلمان الغثبر وسليمان بن عبد العزيز بن هيشة، الاصطياد الالكتروني الأساليب والاجراءات المضادة، فهرسة مكتبة الملك فهد الوطنية، ط1 2009.

- خالد بن سلمان الغثبر ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، فهرسة مكتبة الملك فهد الوطنية، ط1، 2009.

- ستتكيفتش، العربية الفصحى الحديثة بحوث في تطور الألفاظ والأساليب ترجمة وتعليق محمد حسن عبد العزيز، دار الفجر للطباعة، القاهرة مصر، د.ت.

- سوسن زهير المهتدي، تكنولوجيا الحكومة الالكترونية، دار أساة للنشر والتوزيع، عمان الأردن، ط1، 2011، ص 394.

- شحادة الخوري، مجلة مجمع اللغة العربية، التعريب والمصطلح، ج4 دمشق.

- صالح بلعيد، اللغة العربية العلمية، دار هومة، الجزائر، ط1، 2003.

- علي القاسمي، مقدمة في علم المصطلح، مكتبة النهضة المصرية، القاهرة ط2، 1987.

- عامر الزناتي الجابري، إشكالية ترجمة المصطلح ؛ مصطلح الصلاة بين العربية والعبرية أنموذجا، مجلة البحوث والدراسات القرآنية، العدد التاسع، السنة الخامسة والسادسة.

- محمد الديداوي، علم الترجمة بين النظرية والتطبيق، دار المعارف للطباعة والنشر، تونس، د.ط، 1992.

- محمد الديداوي، الترجمة والتواصل، المركز الثقافي العربي، الدار البيضاء المغرب، ط1، 2000.

- محمد رشاد الحمزاوي، المنهجية العامة لترجمة المصطلحات وتوحيدها وتنميطها، دار الغرب الإسلامي، بيروت، ط1، 1986 .

- مراد حميد عبد الله، تطور دلالة المفردات المحدثة في النص اللغوي، مجلة الخليج العربي، العدد 40، العدد(1-2)، 2012.

مذكرة جامعية:

- ترجمة المصطلح التقني من اللغة الانجليزية الى اللغة العربية، دراسة تطبيقية لمصطلحات علم الحاسوب، زكية طلعي، مذكرة ماجستير، جامعة تلمسان 2013-2014.

المصادر والمراجع الأجنبية:

- Maria Terésa Cabra, La terminologie théorie, Méthode et application, Les presses de l'université d'Ottawa, Canada, 1ère édition,1998.

- Peter Newmark, text book of translation, Prentice hall International, 1988.

- Vinay & Darbelnet, Stylistique comparée du Français et de l'Anglais, Edition Didier Paris, 1958.

المواقع الالكترونية:

- www.elebda3.net/2523.pdf

- مسرد مصطلحات أمن المعلومات انجليزي/عربي www.nans.gov.sy

- ويكيبيديا الموسوعة الحرة http://ar.wikipedia.org/wik

الهوامش:

1- شحادة الخوري، مجلة مجمع اللغة العربية، التعريب والمصطلح، ج4، دمشق، ص:811-812.

2- علي القاسمي، مقدمة في علم المصطلح، مكتبة النهضة المصرية، القاهرة، ط2، 1987، ص.68.

3- صالح بلعيد، اللغة العربية العلمية، دار هومة، الجزائر، ط1، 2003.

4- ينظر Maria Terésa Cabra, La terminologie théorie, Méthode et application, Les presses de l'université d'Ottawa ,Canada,1ère édition,1998 ,P.155

5- صالح بلعيد، اللغة العربية العلمية، ص89.

6- ينظر Maria Terésa Cabra, La terminologie théorie, Méthode et application ,P156-157.

7- ترجمة المصطلح التقني من اللغة الانجليزية الى اللغة العربية، دراسة تطبيقية لمصطلحات علم الحاسوب، زكية طلعي، مذكرة ماجستير، جامعة تلمسان، 2013-2014، ص.59.

8 - Peter Newmark, text book of translation, Prentice hall International, 1988, p.46-47.

9 – Vinay & Darbelnet, Stylistique comparée du Français et de l'Anglais, Edition Didier Paris, 1958 , p.47-48.

10- المرجع نفسه، الصفحة نفسها.

11- مراد حميد عبد الله، تطور دلالة المفردات المحدثة في النص اللغوي، مجلة الخليج العربي العدد 40، العدد(1-2)، 2012، ص. 135-162.

12- "إن العرب كانوا يغيرون الأسماء الأعجمية إذا استعملوها فيبدلون الحروف التي ليست من حروفهم إلى أقربها مخرجا وربما أبدلوا ما بعد مخرجه أيضا، والإبدال لازم لئلا يدخلوا في كلامهم ما ليس من حروفهم وربما غيروا البناء من الكلام الفارسي إلى أبنية العرب"، ينظر "المعرب من الكلام الأعجمي على حروف المعجم"، الجواليقي، ص 6-10.

13- حمد عبد الرحمان حمد، عوامل التطور اللغوي؛ دراسة في نحو وتطور الثورة اللغوية، دار الأندلس للطباعة والنشر بيروت لبنان، ط1، 1983، ص 119.

14- محمد الديداوي، علم الترجمة بين النظرية والتطبيق، دار المعارف للطباعة والنشر، تونس د.ط، 1992، ص 175.

15- المصدر نفسه، ص 176.

16- ينظر محمد رشاد الحمزاوي، المنهجية العامة لترجمة المصطلحات وتوحيدها وتنميطها، دار الغرب الإسلامي، بيروت، ط1، 1986، ص 35-55.

17- ينظر عامر الزناتي الجابري، إشكالية ترجمة المصطلح ؛ مصطلح الصلاة بين العربية والعبرية أنموذجاً، مجلة البحـوث والدراســات القرآنيــة، العــدد التاسع، السنة الخامسة والسادسة، ص 333-402.

18- محمد الديداوي، الترجمة والتواصل، المركز الثقافي العربي، الدار البيضاء المغرب، ط1 2000، ص 51-52.

19- سوسن زهير المهتدي، تكنولوجيا الحكومة الالكترونية، دار أساة للنشر والتوزيع، عمان الأردن، ط1، 2011، ص 394.

20- خالد بن سلمان الغثبر ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، فهرسة مكتبة الملك فهد الوطنية، ط1، 2009، ص 57.

21 -www.elebda3.net/2523.pdf

22- ينظر مسرد مصطلحات أمن المعلومات انجليزي/عري، الهيئة الوطنية لخدمات الشبكة مركز أمن المعلومات، www.nans.gov.sy و مصطلحات أمن المعلومات لمركز التميز لأمن المعلومات، المركز العربي لأبحاث الفضاء الالكتروني ACCR، http://coeia.edu.sa

23- خالد بن سلمان الغثبر وسليمان بن عبد العزيز بن هيشة، الاصطياد الالكتروني الأساليب والاجراءات المضادة، فهرسة مكتبة الملك فهد الوطنية، ط1، 2009، ص 46.

24- خالد بن سلمان الغثبر ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، فهرسة مكتبة الملك فهد الوطنية، ط1، 2009، ص 72.

25- المرجع نفسه، الصفحة نفسها.

26- المرجع نفسه، ص.57.

27- خالد بن سلمان الغثبر وسليمان بن عبد العزيز بن هيشة، الاصطياد الالكتروني الأساليب والاجراءات المضادة، ص 80.

28- ويكيبيديا الموسوعة الحرة http://ar.wikipedia.org/wik

29- سوسن زهير المهتدي، تكنولوجيا الحكومة الالكترونية، ص 395.

30- -www.elebda3.net/2523.pdf

31- المرجع السابق، ص 411.

32- ويكيبيديا الموسوعة الحرة http://ar.wikipedia.org/wik

33- أنيس فريحة، نحو عربية ميسرة (بيروت، 1955) ص14، ومن الغريب أن (مونتيل) في (L'arabe moderne, p168) استشهد بما قاله فريحة عن التصعيد وجعله (تضمينا). و(التضمين) بمعناه اللغوي يختلف عن ذلك تماما، وليس هو contenu implicite بالمعنى الواسع الذي فهمه (مونتيل) عن ستتكيفتش، العربية الفصحى الحديثة بحوث في تطور الألفاظ والأساليب، ترجمة وتعليق محمد حسن عبد العزيز، دار الفجر للطباعة، القاهرة مصر، د.ت، ص 159.

انطلاقة شبكات الحاسبات الإلكترونية العالمية.

أ.زينب لمونس

جامعة الإخوة منتوري، قسنطينة 01.

مخطّط البحث: ويعتبر عام 1986 بداية لشبكات الحاسبات الإلكترونية العالمية. التي ازدادت شهرتها بشكل دائم حتى الآن، مع زيادة في عدد مستخدميها بنسب مؤوية شهرياً. وتعتبر الولايات المتحدة الأمريكية الرائدة في هذا المجال، وبلغت حصتها أكثر من نصف شبكات أنظمة الحاسبات الإلكترونية وأكثر من ربع سيل المعلومات. وأصبحت شبكات الانترنيت وسطاً للتواصل والعمل المشترك والراحة عند الناس. وأصبح معها غير القادرين على العمل والمعاقين يملكون "كل العالم تحت أيديهم". وقارن بيل غيتس شبكات الانترنيت بـــ"نظام الأعصاب الإلكترونية الذي يملك القدرة على الاستجابة السريعة لأي تغيير في العالم المحيط وتحليل الأوضاع الراهنة، ومساعدة الناس على اتخاذ قرارات سريعة وصحيحة". من خلال هذه النافذة على العالم الجديد، عالم المعرفة، وعالم تكنولوجيا المعلوماتية الحديثة. وأصبح الإنسان المعاصر غير قادر على تصور نفسه دون شبكات الانترنيت. وتنبأ البعض بأن التطور القريب للشبكات سيلعب في تاريخ الإنسانية الدور الذي لعبه في وقته تطور الإنتاج في المصانع، الذي رافق الثورة الصناعية في القرن الـــ 18. ومثل هذا الاستنتاج جاء في أبحاث "تأثير اقتصاد الانترنيت على أوروبا المعاصرة"، التي أجرتها شركة Henley Centre ، ووفق رأي مؤلفي البحث، أن "ثورة الانترنيت" الحالية تكرر الكثير من التغييرات التي جرت في أوروبا خلال القرن الـــ 18، والفرق فقط في أن تفاعلات الثورة المعلوماتية تجري اليوم أسرع بخمس مرات من سابقتها. وغدت الشبكات العالمية حتى اليوم توحد

أكثر من 143 مليون مستخدم في كل القارات. عبر شبكات الاتصال الهاتفي وكابلات الألياف الضوئية، وقنوات الاتصال عبر الأقمار الصناعية للاتصالات.

تأثير الانترنيت على تطور المجتمعات: غدت المجتمعات في القرن الحادي والعشرين أسيرة لأساليب الخداع والتضليل المعلوماتي الناتج عن تطور الحاسبات الإلكترونية وتكنولوجيا المعلوماتية الحديثة خلال القرن العشرين، التطور الذي فرض على البشرية عالم جديد لم تشهده من قبل، ورافق هذا التطور سيل عارم من المعلومات الصحيحة والملفقة والمضللة في آن معاً، انصبت كلها على العقول البشرية عبر قنوات وشبكات الاتصال المتطورة الحديثة، وترك هذا السيل العارم نتائج غير منتظرة في مختلف المجتمعات المتطورة والنامية على حد سواء. ودخلت المعلوماتية في صلب التفاعلات الاقتصادية والاجتماعية والسياسية بعمق وغدت تمثل "ثورة معلوماتية" شاملة وضعت البشرية أمام تحديات أخطار الصراعات التي باتت تهدد الأجيال الصاعدة بعد أن أطبقت عليها الثورة المعلوماتية في الوقت الحاضر ولا يعرف ما ينتظر الأجيال من أخطار مستقبلية. ورافقت الثورة المعلوماتية مفاهيم وقيم جديدة، فرضت على المجتمعات من خارج المؤسسات المدنية الوطنية المؤثرة في المجتمعات الوطنية وهي التي كانت تسيطر تقليدياً على مختلف نواحي الحياة الاجتماعية والسلوكية للأفراد داخل المجتمع الواحد. وجاءت الثورة المعلوماتية بأفكار جديدة طالت جوهر الفرد وشخصيته وبدأت معها تهتز القيم والتقاليد المتوارثة على وقع سيل المعلومات العالمية الصحيحة والملفقة والمضللة والمخالفة للقوانين الوطنية المنهمرة عليه من كل حدب وصوب لأغراض تحريضية بحتة دون قيد أو حدود، وأظهرت المشكلة حالة من التنافس الفوضوي غير المتوازن بين كل ما هو إنساني وحضاري وثقافي ووطني وعالمي.

الثورة المعلوماتية فجرت الحواجز القائمة بين الشعوب والدول : واستطاعت الثورة المعلوماتية فعلاً تفجير الحواجز القائمة بين الشعوب والدول، وغدت المسارات الإلكترونية تتجاوز الحدود القانونية الدولية القائمة في مختلف دول العالم، ووحدت سبل الاتصال والحوار القائمة بين سكان مختلف مدن العالم وبلغاتهم المتعددة. وأضحت الثورة المعلوماتية واحدة من الأدوات التي تسمح للتطور التاريخي البشري بالخروج من المستويات المعتادة إلى مستويات جديدة لم تكن متوقعة. وجاء ذلك تحت تأثير تقنيات شبكات الاتصال INTERNET (INTERnational NETwork) الأمريكية التي ارتبطت بها أهم مراحل الثورة المعلوماتية خلال القرن العشرين، لأنها كانت شبكات عالمية فعلاً تمكنت من ربط الحواسب الإلكترونية المؤسساتية والشخصية، ووحدت ملايين البشر ومئات الدول اتصالياً، بفضل قدرتها الخارقة على تجاوز الحدود السياسية والجغرافية القائمة بين الدول، وقلصت المسافات الجغرافية الفاصلة بين بني البشر، وقضت على الحواجز التي كانت تعترض سبل الحوار الإنساني في مختلف المجالات العلمية والثقافية والسياسية وحتى مستويات التعليم بكل مراحله.

شبكات الانترنت عامل حيوي في حياة البشر: وأضحت شبكات الانترنت عاملا أساسيا وحيوياً في حياة الكثيرين، حتى أطلق على الجيل الجديد تسمية "الجيل الرقمي"، لأن شبكات الإنترنت مثلت تحديا ثقافيا قاسيا للمسلمين والعرب من بين الكثير من التحديات والهجمات التي يتعرض لها المسلمون والعرب كل يوم وعلى مختلف الأصعدة الحضارية والثقافية والتكنولوجية والعسكرية. ولا يخفى عن أحد ما يتمتع به قطاع المعلومات والاتصالات من جاذبية متزايدة في أدبيات التنمية المعاصرة، إضافة لعوامل الجذب التي زادت من الطبيعة التكاملية لقطاع تكنولوجيا المعلوماتية والحاسبات الإلكترونية الحديثة في الدول الإسلامية والعربية. حتى أضحت شبكات الإنترنت من أهم أدوات خلق وتطوير التفاعل التكاملي على

الصعيد الإسلامي والعربي، وأداة للاتصال والتكامل الاقتصادي في العالمين الإسلامي والعربي. وعلى ضوء الطفرة الحاصلة في عالم الاتصالات والمعلومات في العالم خلال السنوات العشر الأخيرة أصبحت الدول النامية ومن بينها بعض الدول الإسلامية والعربية على قائمة الدول المرشحة خلال السنوات الخمس القادمة لتقديم خدمات تكنولوجيا المعلوماتية للشركات العالمية الكبرى بعد تأثرها بالأزمة المالية والاقتصادية العالمية. الأمر الذي دفع بمصر لتقديم طلب لتسجيل نطاق "دوت مصر" لدي المؤسسة العالمية المسؤولة عن تسجيل الأسماء والأرقام على الشبكة الدولية للإنترنت "الإيكان"، وبهذا تكون مصر أول دولة عربية طلبت تسجيلها في هذا النظام متجاوزة هيمنة الحروف اللاتينية. خاصة وأن مجموعة المواقع العربية هي عملياً أقل عددا من المواقع الإسرائيلية اليوم، لأن إسرائيل تقدمت على العالم في مجال برامج معالجة اللغة العربية وترجمتها، وحققت صناعة البرمجيات الإسرائيلية طفرة كبيرة بعد البداية المتواضعة التي بدأت بخمسة ملايين دولار أمريكي في عام 1984 ووصلت إلى 8.5 مليار دولار في عام 1999 وتجاوزت العشرة مليارات دولار أمريكي فيما بعد. ورافقها تطور الصادرات الإسرائيلية من المنتجات الإلكترونية المتطورة، لتقفز من 9.1 مليار دولار أمريكي في عام 1999، إلى 15.3 مليار دولار أمريكي في عام 2004.

وأظهرت نتائج الأبحاث التي نفذتها وزارة التجارة في الولايات المتحدة الأمريكية أن الإذاعة المسموعة احتاجت إلى 30 عاماً من أجل الوصول إلى ساحة إعلامية بلغت 50 مليون مستمع، وأن الإذاعة المرئية احتاجت لـــ 13 عاماً من أجل الوصول إلى ساحة إعلامية بلغت 50 مليون مشاهد، أما الانترنيت فاحتاجت فقط لـــ 4 سنوات من أجل الوصول إلى ساحة إعلامية بلغت 50 مليون مشترك. وأن حجم المعلومات المرسلة عبر شبكات الإنترنت يتضاعف كل 100 يوم، وزاد عدد مستخدمي شبكات الانترنيت حتى عام 2001 إلى 700 مليون مشترك.

ويعود تاريخ شبكة الانترنيت بجذوره لبداية ستينات القرن العشرين، عندما واجهت وزارة الدفاع بالولايات المتحدة الأمريكية مشكلة إستراتيجية صعبة، تتمثل بإدارة البلاد في حال نشوب صراع نووي مع الاتحاد السوفييتي السابق. ومواجهة إمكانية توجيه ضربة نووية لمركز الاتصالات القومي الأمريكي لتعطيله، وليصبح غير قادر على توفير الاتصالات اللازمة بين القادة العسكريين والقوات الإستراتيجية الأمريكية، ليتمكن الخصم بالنتيجة من تجنب الضربة الجوابية. وعملت وكالة أبحاث مشاريع الصعوبات الخاصة (ARPA) في وزارة الدفاع بالولايات المتحدة الأمريكية، على حل هذه المشكلة. ونتيجة لأعمال البحث التي أجرتها، تمكنت من إنشاء نظام غير مركزي، مؤلف من أجزاء مستقلة عن بعضها البعض، لتبادل المعلومات من خلال مظاريف الاتصال، التي يمكن إرسالها إلى عقدة المستلم بمختلف الطرق (كشبكة عنكبوتيه) باستخدام مختلف قنوات الاتصال. وظهر من خلال العمل وضع مثير يتمثل بأن هذا النظام مثل أسهل طريق لإرسال مختلف المعلومات وهو ما سمي بـــ"البريد الإلكتروني."

انطلاقة شبكات الحاسبات الإلكترونية العالمية: ويعتبر عام 1986 بداية لشبكات الحاسبات الإلكترونية العالمية. التي ازدادت شهرتها بشكل دائم حتى الآن مع زيادة في عدد مستخدميها بنسب مؤوية شهرياً. وتعتبر الولايات المتحدة الأمريكية الرائدة في هذا المجال، وبلغت حصتها أكثر من نصف شبكات أنظمة الحاسبات الإلكترونية وأكثر من ربع سيل المعلومات. وأصبحت شبكات الانترنيت وسطاً للتواصل والعمل المشترك والراحة عند الناس. وأصبح معها غير القادرين على العمل والمعاقين يملكون "كل العالم تحت أيديهم". وقارن بيل غيتس شبكات الانترنيت بـــ"نظام الأعصاب الإلكترونية، الذي يملك القدرة على الاستجابة السريعة لأي تغيير في العالم المحيط وتحليل الأوضاع الراهنة، ومساعدة الناس على اتخاذ قرارات سريعة وصحيحة". من خلال هذه النافذة على العالم الجديد

عالم المعرفة، وعالم تكنولوجيا المعلوماتية الحديثة. وأصبح الإنسان المعاصر غير قادر على تصور نفسه دون شبكات الانترنيت. وتنبأ البعض بأن التطور القريب للشبكات سيلعب في تاريخ الإنسانية الدور الذي لعبه في وقته تطور الإنتاج في المصانع، الذي رافق الثورة الصناعية في القرن الـــ 18. ومثل هذا الاستنتاج جاء في أبحاث "تأثير اقتصاد الانترنيت على أوروبا المعاصرة"، التي أجرتها شركة Henley Centre، ووفق رأي مؤلفي البحث، أن "ثورة الانترنيت" الحالية تكرر الكثير من التغييرات التي جرت في أوروبا خلال القرن الـــ 18، والفرق فقط في أن تفاعلات الثورة المعلوماتية تجري اليوم أسرع بخمس مرات من سابقتها. وغدت الشبكات العالمية حتى اليوم توحد أكثر من 143 مليون مستخدم في كل القارات. عبر شبكات الاتصال الهاتفي، وكابلات الألياف الضوئية، وقنوات الاتصال عبر الأقمار الصناعية للاتصالات.

ومما سرع تطور شبكات الاتصال إنشاء منظمات لإدارة الشبكات العابرة للقارات، ففي عام 1989 أحدثت في أوروبا RIPE (Resaux IP Europeans) لإدارة وتنسيق عمل الشبكات. ومن أجل تنسيق عمل بنية الشبكة العامة لــ Europeans. ومن أجل تنسيق عمل البنية التحتية العامة ركزت الجهود لإعداد وإقرار إجراءات تنظيمية تخدم المنظمة، وتضمنت الأجهزة التالية: الجهاز المركزي IAB (Internet Activities Board) المؤلف من لجنتين تابعتين هما لجنة الأبحاث IRTF (Internet Research Task Force)، واللجنة القانونية IETF (Internet Engineering Task Force). وتعتبر IETF الخدمة الإدارية الأساسية للإنترنيت، وتهتم بمسائل المقاييس وتتخذ القرارات في مجالات مقاييس RFC (Request For Comments). وتتألف هذه اللجنة التابعة من أقسام متخصصة وتقسم إلى فرق عمل وفق المهام. وكل المقاييس التي أقرتها IETF من أجل RFC وضعت في متناول الجميع. وبالإضافة إلى ذلك شملت شبكات الإنترنيت منظمة

حملت اسم(NIC (Network Information Center، تعمل على نشر المعلومات التقنية، وتسجيل وإيصال المستخدمين للشبكات، وإقرار المهام الإدارية مثال: نشر العناوين في الشبكات. أما خدمات الحاسبات الإلكترونية الخاصة للانترنيت في الأقاليم والمنظمات المحلية وبعض الأشخاص فتقدمها خدمة ISP (Internet Service Providers).

المعلوماتية حققت معالجات متقدمة للغة في إطار تطبيق أساليب الذكاء الصناعي: وقد حققت المعلوماتية معالجات متقدمة للغة في تطبيق أساليب الذكاء الصناعي لإعطاء الآلة المهارات اللغوية من اشتقاق، وتصريف، واختصار وفهرسة، وترجمة أولية. وبذلت اليابان جهودا هائلة لكسر عزلتها اللغوية في المعالجة والترجمة الإلكترونية. والجدير بالذكر أن ما نسبته 60% من مستخدمي الإنترنت باللغة العربية في عام 2007 كان في الدول الخليجية العربية، وهذا يرجع إلي أنها واكبت التقنية بشكل مستمر وقامت بتطوير البنية التحتية للإنترنت. بينما انخفضت بشكل ملحوظ في الدول الإفريقية، ولا توجد دولة عربية اليوم إلا وقدمت معلومات حكومية أو خاصة على شبكة الإنترنت. وتمخض عن هذا ارتفاع عدد مستخدمي الإنترنت للناطقين باللغة العربية، وفقا لأحدث إحصاءات عام 2009 ليصل لنحو 50 مليونا ونصف المليون، أي نحو 17.3% من تعداد الناطقين باللغة العربية، و2.9% من تعداد المستخدمين في العالم، وهي المرتبة الثامنة بين لغات العالم الأخرى، بعد اللغة الإنجليزية التي بلغت نسبتها 28.9%، والصينية 14.7%. وتعد تونس أول بلد عربي أدخل الإنترنت حيز الخدمة في عام 1991، بينما كانت الإمارات العربية المتحدة الدولة الوحيدة التي قامت بتوقيع معاهدة التجارة الإلكترونية، لحماية معلوماتها الإلكترونية، وطموحاتها لإيجاد سوق اتصالات مجانية لجميع سكانها بحلول عام 2015.

وتشير بعض التقديرات إلى تراوح عدد مستخدمي الإنترنت في الدول العربية ما بين 10 و12 مليون مستخدم في نهاية علم 2002، وبمقارنتها بعام 2000 تصل نسبة النمو إلى 140%، ويخفي هذا تفاوتا كبيرا بين الدول العربية. ومن الجدير بالذكر أن خريطة مستخدمي الإنترنت في العالم العربي تغيرت تماما في عام 2009.ووفقا لآخر الإحصاءات، تجاوز عدد مستخدمي الإنترنت في العالم العربي الـــ38 مليون مستخدم، وسجلت دولة الإمارات العربية المتحدة أعلى معدل للانتشار بلغ 49.8% من إجمالي عدد سكانها، تلتها دولة قطر 34.8%، ومملكة البحرين 34.7%، وجمهورية مصر العربية 15.9% من إجمالي عدد السكان. وكشفت إحصاءات 2009 عن أن مصر مثلت 18.7% من نسبة المستخدمين في القارة الإفريقية، وإسرائيل 9.2%، وإيران 56.1% بالنسبة للشرق الأوسط، بينما احتلت الصين أعلى نسبة استخدام في آسيا وبلغت 48.8%، تلتها كوريا الجنوبية بنسبة 5.5%. بينما مثلت الولايات المتحدة الأمريكية 13.1% من مستخدمي الإنترنت في أمريكا الشمالية. ومثلت تركيا 6.3% من المستخدمين في القارة الأوروبية. أما نسب ترتيب مراكز الدول على مستوى العالم، فتظهر أن الصين احتلت المركز الأول بنسبة 20.8%، ثم الولايات المتحدة في المرتبة الثانية بنسبة 13.1%، وكوريا الجنوبية في المرتبة العاشرة بنسبة 2.2%، تلتها إيران بنسبة 1.9%، ومن ثم تركيا بنسبة 1.5% لتأخذ المرتبة السابعة عشرة على مستوى العالم. وأوضحت تقديرات عام 2009 أن نسبة مستخدمي الإنترنت في العالم بلغت نسبة 25.6% من عدد سكان العالم، أي أكثر من 6 مليارات نسمة، وبذلك تكون نسبة النمو من عام 2000 وحتى عام 2009 بنحو 380.3%. وبدأت شبكات الحاسبات الإلكترونية عملها في روسيا عام 1986. ودخل المواطنون الروس لشبكات الإنترنيت في نهاية عام 1990. وقدمت خدمات الانترنيت حينها خدمة قيمة لوسائل الاتصال والإعلام الجماهيرية أثناء التمرد الذي

حصل في روسيا عام 1991، لأن شبكات الانترنيت في موسكو لم تكن تحت الرقابة ولهذا استطاعت أن تنشر أخبار إيجابية عن الأحداث الجارية. وخلال أيام التمرد في آب/أغسطس 1991 تم من خلال شبكة الانترنيت نشر 46 ألف خبر لكل أنحاء روسيا والدول الأجنبية. وتتضمن صفحات الانترنيت الروسية اليوم الكثير من الأخبار الهامة والمفيدة وتشمل عملياً كل أوجه حياة المجتمع، ولكن الوصول لخدمات شبكات الانترنيت في روسيا يشمل نحو 3% من السكان. في الوقت الذي كان يتم فيه الوصول إلى الثقافة في ظروف الثورة الاتصالية في العالم العربي عن طريق الإذاعتين المرئية والمسموعة بنسبة 46% وعن طريق شبكة الإنترنت بنسبة 0.026% رغم أن عدد المواقع العربية المسجلة في الانترنيت وصل إلى 41745 موقعا إلا أن نسبة استخدام الإنترنت في دولة الإمارات العربية المتحدة لا يتجاوز الــ 33%، وفي دولة قطر 26%، وفي المملكة العربية السعودية 11%، وفي جمهورية مصر العربية 7%، وفي الجمهورية العربية السورية 7.%.

الشبكات العالمية شكلت عالم الفضاء الواقعي الجديد: وكان تطور الشبكات العالمية سبباً لظهور عالم الفضاء الواقعي الجديد، الذي نمت فيه بشدة عملية تداخل المجتمعات وبعض الشخصيات من مختلف المجتمعات إذ لا توجد حتى الآن توقعات علمية لمستقبل تطور الفضاء العالمي، ولا تتوفر الخبرات لمنظمات الفضاء العالمي بعد. وأمام سعة وصعوبات وتصرفات نظم الفضاء العالمي خرجت تلك النظم عن إطار بداياتها في المشروع الأمريكي منذ زمن بعيد. ويجري اليوم التصدي لحل مسائل الخطوات القادمة لتطوير شبكات الانترنيت. واعتبر مدير تجمع W3C تيم بيرنيرس لي أن طبيعة المرحلة الجديدة لتطور شبكات الإنترنيت تتميز بالعمل المشترك للحواسب الإلكترونية عبر الشبكات دون تدخل الإنسان. ويجري العمل بشكل واسع لترشيد البنية التحتية لشبكات الحاسبات الإلكترونية

العالمية مستقبلاً. وهناك بعض المشاريع لإقامة بنية تحتية موحدة للاتصالات عالية السرعة في القرن الـــ 21 .ومن تلك المشاريع مشروع INTERNET2 الذي أعد بدعم من UCAID (University Corporation for Advanced Internet Development). ويشمل شركات معروفة مثل : IBM, Fore Systems, Cisco, 3Com, بمشاركة الصندوق العلمي القومي، ووزارة الدفاع في الولايات المتحدة الأمريكية. ويخطط للمرحلة الأولى من المشروع توفير سرعة لنقل المعلومات تبلغ 2.4 غيغا بايت في الثانية، وتوحيد شبكات كبريات الجامعات في أمريكا الشمالية والمخابر، ومراكز الحاسبات الإلكترونية. ومن الملاحظ أن مثل هذه المشاريع بدأت اليوم بالتأثير على عمل الفضاء العالمي للقرن الـــ 21. وأن أوروبا لم تزل متخلفة عن اللحاق بالولايات المتحدة الأمريكية في مجال قنوات الاتصال عالية السرعة.

الانترنيت مجال جديد للعمل التجاري: وبالإضافة إلى ذلك كانت شبكات الانترنيت مجالاً جديداً تماماً للعمل التجاري. إذ سمحت للشركات بالعمل بسرعة ودون وسطاء ومن دون استخدام قنوات الاتصال التقليدية عالية التكاليف، ووفرت إمكانيات متساوية للجميع في كل أنحاء العالم، وفرضت حدوداً اقتصادية، ووفرت فرصاً للأمن في عملية تبادل المعلومات داخل المؤسسة الواحدة أو بين مختلف المؤسسات والشركات والمنظمات البعيدة جغرافياً عن بعضها البعض مما وسع دائرة المستهلكين. إضافة للحركة التي وفرتها الشبكة وسمحت من جديدة بالنظر للأشكال الجديدة من الخدمات والبضائع. ومن الأمثلة على ذلك: يمكن من خلال الشبكة في الكثير من دول العالم حجز التذاكر لحضور الألعاب الرياضية والنشاطات الترفيهية، والسفر بالطائرات والسفن والقطارات. ويعمل بنجاح في روسيا نظام للحجز المسبق لبطاقات خطوط السكك الحديدية للسفر على خطوط دول رابطة الدول المستقلة، وبطاقات .(www.express.tsi.ru) ووفر ظهور

التسويق عبر شبكات الإنترنيت إمكانيات جديدة رخيصة، وسريعة، وعملية من خلال الشبكات، لأنه يمكن تجديد صفحات الـــ Web خلال ثوان لا أكثر. وتعتبر بعض صفحات الـــ Web أنه كلما وصلت المعلومات بسرعة للمشترين، كان اتخاذ القرار بالشراء أسرع. ووضع هذا الأسلوب في التسويق قيد الاستخدام من خلال الأبحاث العلمية التي جرت في هذا المجال، وأظهرت الأبحاث أن الكثير من المستخدمين يزورون الصفحات في البداية من أجل التعرف على المنتجات الجديدة وسرعان ما يتخذون قرارات من خلال المعلومات التي يحصلون عليها. وينتظر الخبراء حدوث تطورات كبيرة في مجال التجارة الإلكترونية، التي وفرتها عقد الـــ Web في مجال تجارة المفرق. وصناعة الإعلان والتسويق، التي كانت موجهة للمستهلكين قبل ذلك عن طريق الصحف، والإذاعتين المسموعة والمرئية، إلا أنها بدأت تأخذ ملامحها الخاصة في شبكات الانترنيت، وتطورت معها إستراتيجية التسويق التي أصبحت جديدة تماماً عما كانت عليه في السابق.

نظم الاتصالات الإلكترونية هي نظم جديدة للمدفوعات المالية: ولا يمكن اليوم تصور السوق المالية العالمية دون استخدام نظم جديدة للمدفوعات المالية الإلكترونية. ووفق توقعات المختصين سيستخدم 7 آلاف بنك صفحات الـــ Web الخاصة بهم حتى بداية القرن الـــ 21. وأن عدد البنوك التي تستخدم شبكات الانترنيت في نشاطاتها فعلاً كان لا يتعدى الألفين فقط. وأن الصفقات التي تمت عن طريق شبكات الإنترنيت تمت دون استخدام البنية التحتية للاتصالات التقليدية عالية الكلفة في البنوك. ومن الأمثلة على استخدام البنوك لشبكات الانترنيت البرنامج الجديد الذي أعده ووضعه قيد الخدمة) Nations Bank رابع بنك في الولايات المتحدة الأمريكية)، بعد أن تأكد من عدم فعالية التكنولوجيا القديمة في خدمة الزبائن بالسرعة والنوعية الجيدة. وشمل البرنامج تنظيم خمس مراكز للخدمات المعلوماتية وزعت في مختلف مناطق الولايات المتحدة الأمريكية، بحيث

تمكن أي زبون من الاتصال عن طريق الهاتف أو الانترنيت للتأكد من أوضاع حسابه، والحصول على خدمات البنك. ومن المنتظر مستقبلاً توفير تقديم الخدمات للزبائن عبر الحاسبات الإلكترونية الشخصية، وأجهز الهاتف المزودة بخدمات الصوت والصورة، ومن الأكشاك الخاصة بتلك الخدمات المزودة بأجهزة صغيرة مع شاشات ويمكن من خلالها الحصول على النقود أو صرف الشيكات، ويمكن للزبون الدخول بحوار مع موظفي البنك وتزويدهم بتوجيهاته ومراقبة صحة إملاء الوثائق الضرورية للعملية المصرفية من خلال شاشته. وفي آخر نموذج لتلك الأكشاك المخصصة للعمليات المصرفية يمكن إدارة العملية بكل تفاصيلها من خلال اللوحات المثبتة فيها، والمطلوب من الزبون فقط الضغط بإصبعه على الصورة المطلوبة.

سلبيات التطور التكنولوجي للمعلوماتية: وإلى جانب الايجابيات التي حصلت وتحصل عليها الإنسانية من تطور تكنولوجيا المعلوماتية الرفيعة كشبكات الانترنيت، يواجه العالم جوانب سلبية لهذه الظاهرة منها: التضليل والزيادة العاصفة للجرائم المرتكبة عن طريق الحاسبات الإلكترونية، وخاصة في المجالات الاقتصادية والإقراض المالي. ومن المعلومات التي نشرتها وزارة الداخلية الروسية عام 1997، أن حصة الجرائم المرتكبة عن طريق الحاسبات الإلكترونية بلغت نسبة 0.02 % من عدد الجرائم في المجال المالي. وأن الخسائر المادية بلغت أكثر من 20 مليار روبل. ووفر انفتاح الشبكات إمكانيات أكبر للمسيئين الذين استطاعوا من خلالها الوصول إلى المعلومات الخاصة والسرية، ونسخها وإجراء تعديلات عليها أو حتى إتلافها، إضافة لإمكانية معرفة كلمات السر، وعناوين الصفحات الإلكترونية وغيرها، وحتى الدخول إلى الشبكات بأسماء مسجلة لمستخدمين آخرين. ونتيجة لتلك التصرفات تضررت شركات معروفة بشكل كبير، وتضررت قدرتها التنافسية، وعرضتها لفقدان ثقة الزبائن. مما أضطر شركات الحاسبات

الإلكترونية الكبيرة لتنظيم مجموعات عمل خاصة ذات طبيعة أخلاقية، للتسلل العلني لنظم مختلف الشركات وتحليل نظم الحماية فيها وإعطاء مقترحات لإزالة أماكن الضعف في تلك الأنظمة.

إضافة للأخطار الناتجة عن فصل الموظفين من العمل، لأنهم يملكون إمكانيات كبيرة للوصول إلى عمليات شبكات المؤسسات المفصولين منها، ويعرفون أسرار تركيبتها وحدود حمايتها. وأشار المتخصص بجرائم الحاسبات الإلكترونية المصرفية الفيدرالية في الولايات المتحدة الأمريكية دين نيلسين في كلمته أمام المشاركين في مؤتمر RSA Data Security، إلى مسؤولية "أولائك الناس عن الجرائم وليس طبيعة العمل لأن القسم الأكبر من الجرائم المرتكبة كانت من خلال الحاسبات الإلكترونية للشركات الأمريكية". وأدين جورج ماريو بارنيتيه، تقني الحاسبات الإلكترونية السابق في شركة .Forbs Inc، بالتسلل للشبكات الداخلية للشركة وتخريب ما تحتويه من المعلومات، وأدى تسلله لتوقف خمسة شبكات من أصل ثمانية شبكات عن العمل، وتحمل الشركة خسائر وصلت إلى 100 ألف دولار أمريكي. وأكد مندوبو Forbs أن التخريب التكنولوجي حصل مباشرة بعد فصل بارنيتيه عن العمل. ونتيجة للإجراءات التي قامت بها خدمة جرائم الحاسبات الإلكترونية المصرفية الفيدرالية عثروا في منزل المجرم على معلومات خاصة عن نشاطاتForbs ، ومن ضمنها موازنة قسم تكنولوجيا المعلوماتية لعام 1997 وعدد من قوائم الخدمة الخاصة بنائب رئيس الشركة.

وطالت جرائم التسلل غير القانونية صفحات شبكات الانترنيت لإدارة الأسلحة النووية والأجهزة العسكرية. ومن أخطر الجرائم كان التسلل الذي حدث في أكتوبر/تشرين أول عام 1997 لنظم وكالة المعلومات الخاصة بالدفاع في الولايات المتحدة الأمريكية، وسرقة البرامج العملياتية للرقابة على شبكات المعلوماتية منها. وتستخدم البرامج المسروقة في شبكة نظم الأقمار الصناعية الأمريكية، لتوجيه

الصواريخ إلى أهدافها، وتوجيه القوات البرية والبحرية والجوية ومتابعة تحركاتها وتقديم المعلومات إليها عن الأوضاع المترتبة في مناطق العمليات. ويشمل النظام أماكن تمركز القوات، وإدارة قواعد الدفاع الجوي في كولورادو، وتخدمها عشرات الأقمار الصناعية الموضوعة في مساراتها حول الكرة الأرضية. وتعتبر من أهم القواعد المتقدمة للولايات المتحدة الأمريكية في حال نشوب عمليات عسكرية في الفضاء الكوني.

ومن الأمثلة الأخرى على التسلل لنظم شبكات الحاسبات الإلكترونية. التسلل الذي قام به المواطن الكندي جيسون ميوخيني البالغ من العمر 22 عاماً إلى شبكات المركز الدفاعي لـــ .NASA مما أجبر إدارة المركز على إعادة تنظيم المركز من جديد وتغيير نظمه الأمنية، وبلغت الخسائر الناتجة عن هذا التسلل أكثر من 70 ألف دولار أمريكي. ومن حوادث التسلل الأخرى قيام متسللين روس بأعمال جماعية ضد إدارات الولايات المتحدة الأمريكية، حيث تمكنوا خلال ثلاثة أيام من بدء حرب الناتو ضد يوغوسلافيا من تنفيذ أكثر من 40 عملية تسلل لمراكز الحاسبات الإلكترونية للبيت الأبيض، ووزارة الدفاع، وشبكات اتصالات الحاسبات الإلكترونية في الولايات المتحدة الأمريكية. ووفق ما صرح به المتسللون أن أكثر من ثلثي محاولاتهم لإدخال فيروسات أو تخريب الشبكات تكللت بالنجاح. وأكد متخصصون عاملون في مجالات غزو الفضاء صحة هذه المعلومات. وجاء في تقييماتهم أن عمليات المتسللين لشبكات مراكز الحاسبات الإلكترونية هدفت زعزعة نظم GPS، وجلبت وراءها صعوبات بالغة، في نظم الحاسبات الإلكترونية لملاحة السفن البحرية والطائرات. وتنبؤا بأن مثل هذه الأعمال تستطيع عملياً إخراج النظم الأمريكية لتوجيه الصواريخ والقذائف لأهدافها بالكامل من ساحة العمليات، وهو ما يمكن أن يؤدي إلى كوارث وصراعات عالمية. واعتبر الخبراء أن المتسللين لشبكات مراكز الحاسبات الإلكترونية أرادوا إظهار قدراتهم التي أتاحها لهم التطور

الحاصل خلال قرن المعلوماتية، وإظهار قوتهم ومقدرتهم على التسلل بسهولة إلى أي منظمة حكومية أو أي تجمع كبير للشركات العالمية. وبدوره اعتبر يوجين سبافورد الخبير في الأمن المعلوماتي بجامعة بارديو "أن المتسللين إذا كانوا يحاولون بأعمالهم تلك جذب الانتباه فهم مخطئون، لأن أعمالهم تلك لن تساعدهم على الوصول إلى أهدافهم."

ورافق ظهور شبكات لها مخارج توصلها بقنوات الاتصال المفتوحة، زيادة محاولات التسلل إليها من أي نقطة على الكرة الأرضية. وكل ما تحتاجه توفر مستخدم طفيلي مع حاسب آلي مزود بجهاز اتصال يمكنه من الاتصال بالشبكات. وفي هذا الصدد أعلن تشارلز بالمير، رئيس مخبر الأبحاث العالمية للأمن في شركة IBM. أنه هناك "نحو 100 شخص في العالم لا يرغب بأي شكل من الأشكال أن يصلوا إلى حاسبه الإلكتروني الشخصي. وأنه هناك في الوقت الحاضر نحو 100 ألف متسلل لشبكات الحاسبات الإلكترونية في العالم منهم 9.99% يمكن استخدامهم كمحترفين للمشاركة في عمليات التجسس الصناعي، و0.01% من مجرمي شبكات الحاسبات الإلكترونية على المستوى العالمي. والبقية 90% من هواة استخدام الفضاء المعلوماتي للتسلية.

وأظهرت التحليلات التي أجراها الاقتصاديون أن القوة المحركة الهامة للتحولات في الاقتصاد الإعلامي ترتبط بأربع عوامل اقتصادية، هي: – تكامل الاقتصاد القومي على المستوى الإقليمي مثال: الاتحاد الأوروبي؛ – ونشوء عالم حر يتخلص من الأيديولوجية الأمر الذي يسمح للدول بالعمل المشترك دون تأثير للأيديولوجية؛ – وبروز دور التطور التكنولوجي الذي أدى إلى تطور الاقتصاد العالمي وشجع على المنافسة العالمية. وأن التبدلات الهائلة الجارية في اقتصاد وسائل الاتصال والإعلام الجماهيرية برأي الكثير من الباحثين تشجعها عوامل النظام الاقتصادي الشامل. ولو أن آراء مختلف الباحثين حول العوامل السياسية

والاقتصادية تختلف بشكل واضح، ولكنهم يتفقون على تأثير التكنولوجيا الحديثة على اقتصاد وسائل الاتصال والإعلام الجماهيرية من خلال حقائق واضحة. وأن النتائج التي توصلت إليها التكنولوجيا شجعت على تطوير وإعادة تنظيم الاقتصاد الإعلامي، وخاصة في الآونة الأخيرة التي أضافت عوامل ونتائج محددة جديدة. وليس غريباً أن النتائج المتوقعة في الألفية الجديدة أخذت منحى عالمياً شاملاً. ولكن الغريب في أن الاقتصاد الإعلامي لم يزل يجري قياسه وفقاً للتقارب التكنولوجي لوسائل الاتصال والإعلام الجماهيرية الحديثة التي تتعرض عملياً لإعادة تركيبة الاقتصاد الإعلامي بالكامل مع بروز تناقضات في النظريات السائدة خلال السنوات العشر الأخيرة.

ومن المعروف أن التفاعلات المناهضة للتركيز في وسائل الاتصال والإعلام الجماهيرية كانت قد بدأت بعد الحرب العالمية الثانية ورافقتها دراسات إعلامية قدمت مجموعة من الأبحاث. أدت إلى نشوء اتحادات لوسائل الاتصال والإعلام الجماهيرية فرضت نفسها تحت ضغوط منطق السوق، واعتبرت كاتجاه رئيسي لتطوير الصناعة الإعلامية. بينما أثار عمالقة الإعلام الذين ركزوا في أيديهم الصحافة المطبوعة وقنوات البث الإذاعي المسموع والمرئي، مخاوف كبيرة عند السياسيين وجمهور واسع من الديمقراطية، وتعدد الآراء، وآراء الثقافة السياسية البراقة، واللغوية للأقليات، في الوقت الذي كان يجري تعويضها من خلال الاستقرار والقدرات الاقتصادية لعمالقة الإعلام الجدد. والقضاء على التنوع وتركيز وسائل الاتصال والإعلام الجماهيرية لتقدم صناعة الإعلام موارد كافية وثبات وتقدم ملحوظ. وقدمت التفاعلات مفاجآت غير منتظرة دخلت بنتيجتها للسوق الذي سيطرت عليه المؤسسات الإعلامية الضخمة في الولايات المتحدة الأمريكية وغرب أوروبا لفترة طويلة وخاصة في ثمانينات القرن العشرين ليصبح عامودياً تنخفض معه قيمة الأسهم في الأسواق، وأدى إلى تداعي الأوضاع المادية

للمؤسسات الإعلامية الضخمة. ومن أوائل الاندماجات الضخمة التي جرت خـــلال السنوات الأخيرة: تايم أورنير، وفياكوم، وديزني، الذين اتفقوا على ضرورة نقـــل ثقل نشاطاتهم إلى المجالات التقليدية التي تشـــكلت تاريخيـــاً. وخاصـــة التركيبـــة الإعلامية الجديدة التي تألفت من مستويين ينتظران مـــن الشـــركات المهيمنـــة أن تسيطر على 80 أو 90% من الموارد، مبقية للإنتاج المساعد نحو 20% فقط.

التغييرات الاستراتيجية الحديثة في مجال الإعــلام: ومـــن هـــذه التغييـــرات الاستراتيجية الحديثة التي طالت نشاطات الكثير من الشركات المعروفـــة، شـــركة الإعلام والترفيه ديزني. وفي مقابلة أجرتها صحيفة فايننشيل تايمز مع مدير شركة الإعلام والترفيه ديزني م. إيسنير، تحدث عن تلك التغييرات، واعترف بأن النتائج المالية خلال العام ستكون سيئة في أحسن الأحوال كما في السابق، وأشار إلـــى أن الاهتمام المتواضع الذي ستبذله الشركة سيوجه إلى مضامين الإنتاج. وأن ديزنـــي غير مهتمة بشراء محطات جديدة للإذاعة المسموعة والمرئية، ولكنها ستتجه نحو خلق توازن لمواجهة الإستراتيجية السابقة للفروع العاملـــة فـــي مجـــال تطـــوير الانترنيت والتجارة الإلكترونية. وأوجد نموذج السوق الجديدة وزناً مضاداً لعمليـــة الإنتاج المتجهة نحو السوق السابقة التي حرمها الاندماج من الموارد وأسهم فـــي تبذيرها، وأضعفت ظروف التقارب إمكانيات الشركة. لنرى أن التقـــارب فـــرض على المنشآت الإعلامية إتباع إستراتيجية مرنة لتحقيق الثبات في الأسواق. وتطرق الكثير من الباحثين الغربيين إلى فكرة أن التقارب سيؤدي إلى تقاسم الأسواق، وإلى التحول من الصناعات التقليدية التي تحافظ على تقسيم وسائل الاتصال والإعـــلام الجماهيرية، الصحف، والبث الإذاعي المسموع والمرئي، والكابلات، إلـــى إنتـــاج منتجات جديدة تشمل تكنولوجيا الاستعمال اليومي وتقنياتها، وإنتاج منتجات تـــدعم قنوات التوزيع. وأدى ظهور أنواع جديدة مـــن منتجـــات صـــناعة المعلوماتيـــة والاتصال، بغض النظر عن التغييرات المستمرة إلى تشكل طليعة جديدة، في مجال

إنتاج المضامين (المنتجات ذات المضمون الإعلامي) للإذاعة المرئية لتبقى الطليعة لكبار التقليديين أمثال: ديزني/إيه بي سي؛ وأونيـر؛ وإن بـي سـي؛ وفـوكس. وفي مجال إنتاج منتجات المضمون الإعلامي للسينما ظهـرت نفـس الشـركات: ديزني؛ وبياكوم؛ وتايم أونير. وبقيت الطليعة للإذاعة المسموعة للشركة المعروفة : فيستينغاوز. ومن السهل ملاحظة أن الأوضاع التاريخية للإعلام المعروفـة فـي القطاعات الجديدة بقيت قريبة من السنوات العشـر السـابقة. وحملـت الطليعـة الاقتصادية للشركات البارزة بالكامل الصفات التقليدية لتركيبة السوق والسـيطرة. ومع ذلك تبقى مراحل تطور التقارب في الأسواق في النهايـة داعمـة لقـدرات وسيطرة عدد محدود من اللاعبين على الساحة الإعلامية. وأدى التقارب إلى تغيير أساليب التكنولوجيا الإعلامية، وفي المضمون الإعلامي، وفي الأسواق الإعلامية. وبشكل أقل بقيت تأثيراتها على تغيير علاقات السياسيين مـع مـا يجـري مـن تغييرات. وأول استجابة للسياسيين على تفاعلات التقارب كانت بظهـور قـوانين جديدة موجهة نحو ليبرالية أسواق الإعلام والاتصالات وتشجيع المنافسة فيها. وإلى إضعاف الاحتكارات السابقة في أسواق الاتصالات تمكن بعـض الشـركات مـن دخول الأسواق، وتخفيض الأسعار، وتقريب كـل قطـاع الخـدمات المعلوماتيـة والاتصال الحديثة من المستهلكين.

ويبقى التقارب جزئياً في فن الخطابة وأساليبها في المراكز السياسـية للـدول البارزة في العالم، وبالدرجة الأولى الولايات المتحدة الأمريكية والدول الأعضـاء بالاتحاد الأوروبي. ومنها خطاب قانون الاتصالات في الولايات المتحدة الأمريكية لعام 1996، والكتاب الأخضر للتقارب الذي وافق عليه الاتحـاد الأوروبـي فـي ديسمبر/كانون أول عام 1997، التي بقيت حتى الآن من أشهر الوثائق السياسـية التي تدعوا لتشجيع التقدم في التقارب على المستوى السياسي. وانطلقت الـوثيقتين من المبادئ القديمة لتنظيم وسائل الاتصـال والإعـلام الجماهيريـة الإلكترونيـة

المضطرة للتعامل مع مشاكل تحديد الموجات الإذاعية المسموعة والمرئية. ولو أن التقارب يلغي هذه المشكلة بحيث لن يضطر الوسط المعلوماتي والاتصالات الجديد لتوزيع الموجات الإذاعية المسموعة والمرئية بعد أن أصبحت وسائط للعمل المشترك في القنوات والمضامين الإعلامية الجارية بتناقض مع نظم القوانين التقليدية، مبنية على تحديد نشاطات مشغلي الشبكات، والإذاعتين المرئية والمسموعة. وليصبح الوصول الحر إلى شبكات نظم الاتصالات الحديثة بالكامل خاضع للسياسات الجديدة للدول إضافة لـ "الأشخاص العاملين" على تحديد أسعار الوسائط لينمو التقارب بشكل ملحوظ، ويصبح الدور النشيط لمشغلي الشبكات ووسائط الوصول، ومنتجي المضامين الإعلامية والمستخدمين في تحديد أوضاعهم الخاصة.

ويعتبر تأمين فرص الوصول من أهم الاتجاهات السياسية اليوم، ويرافق تقارب الأسواق التخفيف من التركيز والاحتكار الذي يمكن الكثير من الشركات الصغيرة من العمل بنجاح في السوق الإعلامية الحديثة. ناهيك عن أن التخلف عن التقدم التكنولوجي قد يصبح عائقاً جدياً للوصول إلى البنية التحتية العالمية للمعلوماتية والاتصالات في عدد من الدول لا بل ومناطق كاملة من العالم أثناء تكاملها مع البنية التحتية العالمية للمعلوماتية والاتصالات. ويصبح وصول أشخاص محددين للإعلام المتقارب صعب بسبب إمكانياتهم المادية، أو بسبب الأمية التكنولوجية. لأن عملية التقارب الإعلامي اليوم تحتاج لأموال ومعارف جديدة للأشخاص العاديين وموارد كبيرة وإرادة سياسية من الدول والتكتلات السياسية. ومن المعروف أن حقيقة توافق تفاعلات التقارب التكنولوجي لوسائل الاتصال، والتقارب الاقتصادي في الأسواق. توفر لمشغلي الاتصالات دخول سوق شبكات التوزيع بالكابلات وينصهر معها دور النشر مع شركات أفلام الفيديو. ويظهر منتجي البرامج العملية اهتماماً بشبكات الإذاعة المرئية. ليحدث نوعاً من المستويات المتعددة للتفاعل مع

اتحادات الاتصال التي تصبح منجذبة نحو الصناعات التقليدية لوسائل الاتصال والإعلام الجماهيرية، من: الصحافة المطبوعة، والبث الإذاعي المسموع والمرئي والعمل التجاري في مجال الاتصالات. ولو أن الحياة الواقعية مختلفة بين المتنافسين تكنولوجياً في مجالات الاتصالات الهاتفية والإذاعة المرئية، رغم أنهم احتفظوا ولوقت محدد بدورهم بالكامل إلا أنه من الواضح هناك ضرورة لإعداد سياسة اتصالات موحدة.

ولاحظت السياسة الحديثة لليبرالية سوق الاتصالات في سوق الاتحاد الأوروبي دقة الفصل بين البنية التحتية لإعطاء المعلومات والوصول للمضامين، والخدمات التي تقدمها من خلال البنية التحتية هذه. وراعى الكتاب الأخضر للتقارب الصادر عام 1997 الفرق بين النقل عبر وسائل الاتصال والإعلام الجماهيرية التقليدية أو التوزيع، وتقديم الخدمات مع مضامين إعلامية. ولكن في ظروف التقارب التكنولوجي يبقى الضمان الواقعي لتنوع المضمون ممكن فقط في حال خلق الظروف الملائمة لجميع اللاعبين، والعاملين في مجالات التقارب الاتصالي وفي الأسواق الإعلامية، ومشغلي الشبكات، وعقد التوصيل في الانترنيت، ومنتجي مواد المضمون الإعلامي، وخدمات الأشخاص الكثيرين العاملين الذين يحتاجون لوصول متساوي لنظم الاتصال.

ويبقى التقارب التكنولوجي الجاري تطبيقه بالمعنى الملموس عبارة عن "إعادة توزيع للأدوار" في وسائل الاتصال والإعلام الجماهيرية التقليدية، وتغيير الأدوار على ساحة المستفيدين، من كتلة سلبية إلى كتلة ايجابية، تستهلك المضامين المقدمة لها، وتتحول إلى مجموعات محددة بالكامل، من حيث الاستهلاك المعلوماتي للاتصالات المعتاد عليه ويمكن تحديد أطرافها بدقة. ليحظى الجمهور الإعلامي من خلال التقارب مع وسائل الاتصال والإعلام الجماهيرية بخاصية رئيسية كما يجري اليوم. والإعلام الدولي النشيط الجديد يقدم للمستهلكين التقليديين وسائل الاتصال

والإعلام الجماهيرية بإمكانيات غير محدودة لاختيار المضمون. ولكن في الوقت ذاته نرى أن مستخدمي "الأون لاين ميديا" يصبحون مشاركين في تحرير المواد وحتى في إدخال مواد ومضامين جديدة .ليجري من خلالها توحيد المستخدم والمنتج وتؤدي إلى تقارب مختلف الأدوار والوظائف، بدلاً من التقسيم. فالمستخدم المحدد يتحول إلى أحد الحقائق التي هي فعلاً توجه عملية التقارب. ويتحول معها وصول المستخدم في الإعلام الجديد إلى مجموعة من المشاكل التي يتميز بها عصر التقارب، وتجاوزها ممكن من خلال تعاون اللاعبين الكبار في سوق الاتصالات والدولة والقطاع الخاص ومن خلال مساهمتهم النشيطة والفاعلة وبمشاركة المستخدمين لاختيار الدور الإنساني والاجتماعي والاقتصادي وإيجاد الضمانات القانونية للوصول إلى التكنولوجيا الجديدة وشبكات الانترنيت.

ومنه نستنتج أن توقعات اختفاء الصحف أمام منافسيها السينما والإذاعتين المسموعة والمرئية لن يتحقق في عصر الانترنيت لأن الأسباب الحالية هي أكثر تعقيداً من السابق. وتفاعلات تقارب وسائل الاتصال والإعلام الجماهيرية فتحت الطريق عملياً أمام الكثير من الآفاق التي لم تكن معروفة من قبل، وستؤدي لنفس النتائج السلبية أو أكثر. ومن دون الإرادة السياسية في الدول القومية ومن دون تجديد الإسهام النشيط للتجارة الإلكترونية، ومن دون المستوى العالي والنشيط للساحة الإعلامية يمكن أن يبقى التقارب إمكانية فقط وهي الإمكانية التي تحدث عنها الباحثون على عتبة القرن الجديد.

مصطلحات ومبادئ الأمن المعلوماتي الدولي: وتنطلق أهمية المصطلحات المستخدمة من المبادئ التالية:

1- المجال المعلوماتي: وهو مجال النشاطات التي تؤدي إلى صناعة المعلومات ونشرها واستخدامها، ومن ضمنها المعلومات الشخصية والاجتماعية، والمعلومات واستخدام البنية التحتية للاتصالات الهاتفية، والمعلومات الخاصة.

2- الموارد المعلوماتية: وهي البنية التحتية للمعلوماتية (الأجهزة، والنظم المحدثة، والتعامل، وحفظ، ونشر المعلومات) ومن ضمنها الصفحات الإلكترونية وبنوك المعلومات، والمعلومات الخاصة، وسيل المعلومات.

3- الحروب المعلوماتية: المواجهات الحاصلة بين الدول في مجالات المعلوماتية، مثال إلحاق الضرر بنظم المعلوماتية، وعمليات تبادل المعلومات والموارد الحيوية للأجهزة الهامة، وتخريب النظم السياسية، والاقتصادية والاجتماعية، والسيطرة على الحالة النفسية العامة للسكان، وإلحاق الضرر باستقرار المجتمع والدولة.

4- الأسلحة المعلوماتية: وهي الطرق والوسائل المستخدمة من أجل إلحاق الضرر بنظم المعلوماتية وعملياتها ومواردها، والقيام بأعمال سلبية للتأثير المعلوماتي على الدفاع الوطني، والإدارة السياسية، والاجتماعية، والاقتصادية وغيرها من الأجهزة الهامة لحياة الدول، والسيطرة الأوضاع النفسية العامة للسكان، بهدف ضرب استقرار المجتمع والدولة.

5- الأمن المعلوماتي: وهو حماية المصالح الحيوية للأفراد، والمجتمع والدولة، في مجال المعلوماتية، ومن ضمنها البنية التحتية للمعلوماتية والاتصالات الهاتفية، وحماية المعلومات الخاصة، ومقاييسها، وإيجابيتها بالكامل، والوصول إليها، وسريتها.

6- تهديدات الأمن المعلوماتي: وهي العوامل التي تهدد مصالح الأفراد والمجتمع، والدولة، في مجالات المعلوماتية.

7- الأمن المعلوماتي الدولي: وهو أوضاع العلاقات الدولية، التي تهدد الاستقرار العالمي، وترافقها تهديدات لأمن الدول، والمجتمع الدولي، في مجالات المعلوماتية.

8- الاستخدام المخالف للقانون: لـنظم المعلوماتيـة، والاتصـالات الهاتفيـة والموارد المعلوماتية دون الحصول على موافقـة أو مخالفـة القواعـد المتبعـة والقوانين، أو مبادئ القانون الدولي.

9- التدخل غير الشرعي: في النظم المعلوماتية، والاتصالات الهاتفية، والموارد المعلوماتية، والتدخل في عمليات جمع، والتعامـل، وتخـزين، وحفـظ، وتقـديم والبحث، ونشر، وتداول، واستخدام، المعلومات بهدف تخريب العمل الطبيعي لنظم المعلوماتية، أو التسلل للوصول إلى الموارد المعلوماتية السرية.

10- النظم الهامة لحياة الدول والأجهزة والمؤسسات، وهو التدخل المقصود في الموارد المعلوماتية المؤثرة مباشرة على الأمن القومي (النقل، والطاقة، والماليـة والقروض، والاتصالات، وأجهزة الإدارة الحكومية، وإدارات الـدفاع، وأجهـزة الأمن، والموارد المعلوماتية الاستراتيجية، وأعمال منظمات البحث العلمي والتقني لزيادة الأخطار التكنولوجية والبيئية، وأجهزة مواجهة الحالات الطارئة.

11- الإرهاب المعلوماتي الدولي: وهو استخدام الاتصـالات الهاتفيـة ونظـم المعلوماتية ومواردها أو التأثير عليها في مجالات المعلوماتية الدولية بهدف القيـام بأعمال إرهابية.

12- الجريمة المعلوماتية الدولية: وهي استخدام الاتصـالات الهاتفيـة ونظـم المعلوماتية ومواردها أو التأثير عليها لأهداف تخـالف القـانون فـي مجـالات المعلوماتية الدولية.

ويعتمد الأمن المعلوماتي على المبادئ التالية:

المبدأ الأول ويشمل:

1- نشاطات الدول وغيرها من الأطراف الدولية فـي مجـالات المعلوماتيـة الدولية يجب أن تشجع التطور الاجتماعي، والاقتصادي، وفقاً لمتطلبـات الحفـاظ على الاستقرار والأمن العالمي، ومراعاة استقلال غيرها من الـدول، ومصـالح

الأمن، ومبادئ التسوية السلمية للمشاكل والصراعات، وعدم اللجوء إلى القوة وعدم التدخل بالشؤون الداخلية، ومراعاة حقوق وحريات الإنسان.

2- وهذه الأعمال يجب أن تتم وفقاً لحقوق كل إنسان بأن يطلب، ويحصل وينشر، المعلومات، والآراء، التي تضمنها وثائق الأمم المتحدة، مع مراعاة حصر هذا الحق بالنظم القانونية الوطنية بهدف حماية مصالح وأمن الدولة.

3- ويجب أن تحظى أي دولة أو أي طرف من أطراف العلاقات الدولية بحق المساواة لحماية الموارد المعلوماتية وأجهزة حياتها الهامة من الاستخدامات غير القانونية أو التدخل المعلوماتي المخالف للقانون، وأن تعتمد على دعم المجتمع الدولي من خلال استعمالها لهذا الحق.

المبدأ الثاني: امتناع الدول من خلال سعيها لمنع التهديدات في مجال الأمن المعلوماتي الدولي، عن: - الإعداد، وإقامة واستخدام وسائل للتأثير أو إلحاق الأضرار بالموارد المعلوماتية ونظم الدول الأخرى؛ - استخدام المعلومات من أجل التأثير على الأجهزة الهامة لحياة الدولة الأخرى؛ - استخدام المعلومات من أجل تحطيم النظم السياسية، والاقتصادية، والاجتماعية لغيرها من الدول، والسيطرة النفسية على السكان بهدف إشاعة حالة من الفوضى وعدم الاستقرار في المجتمع؛ - التدخل غير المصرح به في نظم المعلوماتية والاتصالات الهاتفية والموارد المعلوماتية، واستخدام هذه النظم والمجالات بشكل غير قانوني؛ - محاولة الدخول والسيطرة على مجالات المعلوماتية؛ - منع الوصول للتكنولوجيا المعلوماتية الجديدة وخلق أوضاع تمنع الدول الأخرى من الوقوع في تناقضات مع مصالحها وتبقيها تابعة للغير في مجال المعلوماتية؛ - دعم نشاطات الإرهاب الدولي والحركات الانفصالية والمنظمات والمجموعات الإجرامية، أو بعض الخارجين عن القانون، الذين يهددون الموارد المعلوماتية، أو الأجهزة الهامة لحياة أي دولة من دول العالم؛ - وضع وتنفيذ خطط وبرامج، تتطلع لإمكانية إثارة

الحروب المعلوماتية وتهيئ الظروف لخلق سباقـــات التسلـــح وتدعوا لخلق حالـــة من عدم الاستقرار في العلاقات الدوليـــة، وتهيـــئ الظـــروف للقيـــام بـــالحروب المعلوماتية؛ – استخدام التكنولوجيا ووسائل المعلوماتية لإلحاق الضـــرر بحقـــوق وحريات الإنسان في مجال المعلوماتية؛ – نشر المعلومات عبر حدود الدول بشكل مخالف لمبادئ الحقوق الدولية أو القوانين النافذة في دول بعينها؛ – السيطرة علـــى سيل المعلومات، ونشر الأنباء المضللة والمختلقة، بهدف زعزعة الأوضاع النفسية والمعنوية في المجتمع، وتخريب القيم والتقاليد الثقافيـــة، والمعنويـــة، والأخلاقيـــة والجمالية؛ – التدخل المعلوماتي والســـيطرة علـــى البنيـــة التحتيـــة للمعلوماتيـــة والاتصالات الهاتفية لغيرها من الدول، ومنعها عن العمل وأداء وظيفتهـــا علـــى الساحة المعلوماتية الدولية.

المبدأ الثالث: توفر منظمة الأمم المتحدة وأجهزتها المختصة الظروف للتعـــاون الدولي، في مجال منع تهديدات الأمن في مجالات الســـاحة المعلوماتيـــة الدوليـــة ووضع القواعد القانونية اللازمة من أجل: – تحديد طبيعـــة وتصـــنيف الحـــروب المعلوماتية؛ – تحديد طبيعة وتصنيف الأسلحة المعلوماتية والطرق والوسائل التي يمكن اعتبارها أسلحة معلوماتية؛ – الحد من تجارة الأسلحة المعلوماتيـــة؛ –منـــع إعداد ونشر واستخدام الأسلحة المعلوماتيـــة؛ – التصـــدي لتهديـــدات الحـــروب المعلوماتية؛ – مساواة تهديدات استخدام الأسلحة المعلوماتية ضد الأجهزة الهامـــة للحياة، بتهديدات استخدام أسلحة الدمار الشامل؛ – تهيئة الظروف من أجل التبادل المتساوي والآمن للمعلومات على الساحة الدولية من خـــلال المبـــادئ والقواعـــد الدولية المعترف بها؛ – منع استخدام تكنولوجيا ووســـائل المعلوماتيـــة لأهـــداف إرهابية وغيرها من الأهداف الإجرامية؛ – منـــع اســـتخدام تكنولوجيـــا ووســـائل المعلوماتية من أجل التأثير على الوعي الاجتماعي، وإشـــاعة حالـــة مـــن عـــدم الاستقرار في المجتمع والدولة؛ – إعداد إجراءات للتعاون المشترك في مجال تبادل

المعلومات ومنع الاستخدامات غير المشروعة للمعلومات من أجل التـأثير علـى غيرها من الدول؛ – إحداث نظم دولية للرقابة ومتابعة التهديدات فـي المجـالات المعلوماتية؛ – إحداث آليات للرقابة على احترام نظام الأمن المعلوماتي الدولي؛ – إحداث آليات لتسوية حالات الصراعات في مجالات الأمن المعلوماتي؛ – إحـداث نظم دولية للترخيص في مجالات المعلوماتية وتكنولوجيـا ووسـائل الاتصـالات الهاتفية (وضمنها التقنيات وبرامج الاستخدام (بهدف ضمان الأمن المعلومـاتي؛ – إحداث نظم دولية للتعاون بين الأجهزة الأمنية من أجل منع ومحاربة الجريمة في المجالات المعلوماتية؛ – إجراء تعديلات طوعية في القوانين الوطنية لتتلاءم مـع ضرورات توفير الأمن المعلوماتي.

المبدأ الرابع: تحمل الدول وغيرها من أطراف العلاقات الدوليـة المسـؤولية الدولية لقاء نشاطات في المجالات المعلوماتية تقوم بها أو يقوم بها الغيـر تحـت غطائها القانوني، أو ترعاها منظمات دولية تنتسب إليها.

المبدأ الخامس: تسوية الخلافات الناشئة بين الدول أو بين أطـراف العلاقـات الدولية، من خلال القواعد الدولية، وبالإجراءات السلمية المعترف بها دولياً.

معززات الجريمة الإلكترونية وواقع الأمن المعلوماتي

أ. محمد الهادي عايش
جامعة منتوري، قسنطينة 1

ملخص المداخلة: تسعى هذه الدراسة للتّعرف على أحد التحديات التي يواجها العالم، المتجسدة في **الأمن المعلوماتيّ**، إذ أن الجرائم المعلوماتية باتت ظاهرة لها تأثيراتها الأمنية والاقتصادية والسياسية وحتى العلمية، هذه التأثيرات كانت نتاجا لتطور تقني عالمي سعت فيه الدول للاستثمار في مجالات تقنية المعلومات من أنترنت وشبكة عنكبوتية وغيرها قصد تطوير الإنتاج ورفع حدة التنافس العلمي ولاقتصادي، وعلى النقيض من هذا برز الوجه السلبي لاستخدام التقنية من اختراقات وجرائم إلكترونية.

مما تقدم بدر إلى أذهاننا فكرة مفادها دراسة عينة من أصحاب مهارة الاختراق وممن لهم ضلوع في جرائم إلكترونية قصد معرفة معززات ودوافع هذا العمل وهل له علاقة بالسرقات العلمية، كما أنه تم التفكير في دراسة مجموعة من تقنيي الحماية الهدف منها معرفة معززات الجريمة الالكترونية، أهم المشاريع التي سيّواجهون بها عملياتهم، وهل هناك إمكانية للحد منها، ببساطة معرفة واقع الامن المعلوماتي من أفواه أهله ومن مخالب مهدديه.

ماهي معززات الجريمة الالكترونية ؟

وماهي سبل الوقاية منها ؟

ما هو واقع الأمن المعلوماتي ؟

الكلمات المفتاحية: الجريمة الإلكترونية، الاختراق (الهكر) الأمن العلوماتي.

عناصر المداخلة:

- **مقدمة اجرائية**

I.المعالجة النظرية للدراسة

تم تقسيم هذه الورقة البحثية إلى المحاور الأساسية التالية:

المحور الأول: الخلفية المعرفية للأمن المعلوماتي والجريمة الالكترونية

- مقدمة إجرائية

- تحديد المفاهيم (الأمن المعلوماتي، الجريمة الإلكترونية، التقنية، السرقة العلمية ..)

II. المعالجة الميدانية للدراسة: تهدف الدراسة في إطارها الميداني إلى التعرف على معززات الجريمة الإلكترونية، وذلك بمقابلة فئة من أصحاب المهارة في الاختراق، والذين لهم سجل حافل بالاختراقات الدولية، الهدف منها معرفة دوافع الاختراق، مستوياتهم، معرفة علاقتهم بالسرقات العلمية، معرفتهم بالقوانين الردعية وغيرها، كما أنه ستكون هناك مقابلة مع تقنيي للحماية لمعرفة سبل الوقاية من الجريمة الإلكترونية.

1- المنهج المستخدم.

2- أداة الدراسة.

3- مجتمع وعينة الدراسة.

4- عرض وتحليل البيانات.

5- خاتمة: فيها أهم النتائج.

مقدمة: تميز القرن الواحد والعشرون باستخدام المعلومات، حيث وسمت عقوده الثلاثة الماضية بأنها عصر الثورة المعلوماتية، فهي فترة شهدت انتشار الكومبيوتر، وتوسع الأنترنت وباقي تقنيات تكنولوجيا المعلومات، مسهلة بذلك حياة الأفراد والدول والمجتمعات، قد حصرت هذه الثورة في أربعة تغيرات سريعة أساسية على الأقل:

الأولى: القفزة الرهيبة لتكنولوجيا الحوسبة.

الثانية: التطور غير المسبوق في تراكم المعرفة.

الثالثة: الأنترنت شبكة جمعت العالم كله في قرية صغيرة

الرابعة : العواقب والتأثيرات الأكيدة والممكنة، والمحتملة التي يتركها ذلك في حياة البشرية اقتصاديا، سياسيا وثقافيا وعلى النقيض من ذلك، تفاقم التيار المعاكس الذي يحاول وبنفس التقنيات تعكير الأجواء وتبديد الاحلام، وفي وريقات هذا البحثً قصدنا الوقوف على الجريمة الالكترونية وواقع الأمن المعلوماتي، وما هدفنا في عملنا هذا إلا خطوة اجتهادية في تعريف وتمييز الجرائم الالكترونية عن غيرها وتأثيراتها على مستوى المجتمع والفرد وما يتوجب فعله للتصدي لها ولتحجيم تأثيرها، وقد تم التطرق في هذا البحث أيضا إلى المحفزات والاسباب وراء ارتكاب هذه الجرائم، وواقع الامن المعلوماتي، مركزين على انتقال الجريمة من العالم الواقعي إلى العالم الافتراضي، وما ينتج عن الفضاء الالكتروني من أنواع جديدة من الجريمة تسمى الجريمة الالكترونية التي أصبحت لها أنماط جديدة من الجريمة منها لصوص الحاسب الذين يدخلون إلى أنظمة الحاسوب وبيانات المعلومات ويسرقونها أو يعبثون بها والجرائم التي تخترق الحماية الأمنية وغيرها.

1- تساؤلات الدراسة:

- ماهي معززات الجريمة الالكترونية ؟
- ما هو واقع الأمن المعلوماتي ؟

2- أهداف الدراسة:

- محاولة فهم الثورة المعلوماتية وآثارها السلبية والايجابية في حياتنا الاجتماعية والثقافية. واستشراف آفاقها الممكنة.

- توضيح فاعلية استخدام التقنية الحديثة لمواجهة مهددات الأمن المعلوماتي.

- الكشف عن المعوقات التي تحد من فاعلية استخدام التقنية الحديثة في مواجهة مهددات. الأمن المعلوماتي.

- التعرف على مصادر مهددات الأمن المعلوماتي.

- التعرف على معززات الجريمة الالكترونية.

- التعرف على سبل الوقاية منها.

3- أهمية الدراسة:

- تبرز الأهمية العلمية لهذه الدراسة في دور التطورات التقنية في ظهور مهددات جديدة وجب الحماية منها.

- تبحث هذه الدراسة عن سبل الوقاية من المهددات المعلوماتية بمعرفة معززات الجريمة الإلكترونية.

4- تحديد المفاهيم:

أ- **تعريف الجريمة الالكترونية:** عند تحديدنا للمفاهيم ارتأينا أن لا نفرق بين الجريمة المعلوماتية والجريمة الإلكترونية وإن كانت الجريمة الإلكترونية أوسع وأشمل.

في البداية الجريمة "هي كل فعل أو نشاط يتم بطريقة غير مشرعة[1]"

أما في ما يخص الجريمة المعلوماتية أعطيّ عدد لا بأس به من التعاريف التي تتباين حسب نوع الجريمة المرتبطة بالمعلوماتية، سواء ارتكب في مجال معلوماتي مغلق أو مفتوح، على الشبكات المعلوماتية، إذ أنه إلى حد الآن لا يوجد تعريف ثابت جامع ومتكامل متفق عليه فالملاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها الغش المعلوماتي، أو الاختلاس المعلوماتي أو الجريمة المعلوماتية.[2] ونظرا لصعوبة إعطاء تعريف لهذه الظاهرة الإجرامية وذلك حصرها في مجال ضيق.

ولقد تباينت الآراء حول تعريف الجريمة الالكترونية حيث يمكن تصنيفها إلى أربعة تعاريف:

1- تعريفات مرتكزة على وسيلة ارتكاب الجريمة.

2 - تعريفات مرتكزة حول موضوع الجريمة.

3- تعريفات مرتبطة بتوافر المعرفة بتقنيات الجريمة.

4 - تعاريف مختلطة ومتنوعة:

ونركز في بحثنا هذا على هذا التعريف التي تقترحه مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية كأساس للنقاش في اجتماع عقد بباريس 1983 لبحث الإجرام المرتبط بالمعلومات مقتضاه أنها كل سلوك غير شرعي أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات[3]. برغم اتساعه البالغ كما يقول البعض، إلا أننا نتخذه كمفهوم إجرائي لبحثنا.

ب- الأمن المعلوماتي:

***مفهوم المعلومات :** فالمعلومات هي أغلى ما يمتلكه الإنسان في حياته على مر العصور لذا سعى إلى جمعها وتسجيلها على وسائط حفظ مختلفة بدء من جدران المقابر والمعابد وأوراق البردي في عصر الفراعنة **إلى** أن تم اختراع الورق في الصين، وتعتبر المعلومات رمز من رموز الحضارة الإنسانية على مدى لتاريخ، وإذا فقد الإنسان معلوماته فهذا يعني فقدانه لذاكرته ومن ثم تضيع حضارته.

والمعلومات من حيث المصطلحات التي تكاد تفقد وزنها الدلالي من كثرة الاستعمال وهي من الكلمات المراوغة صعبة المراس حيث أن جميع التعريفات التي ذكرت في المعلومات تعبر بشكل كبير عن آراء ووجهات نظر أصحابها وهذه التعريفات قد تكون مقبولة عند بعض التخصصات ومرفوضة عند البعض الآخر.

والمعلومات أصبحت في بيئة اليوم ترتبط بمختلف جوانب الحياة، وتمثل ركيزة نشاط الإنسان الاقتصادي والاجتماعي والثقافي والسياسي، وتتيح له المعرفة بالواقع ومشكلاته وأبعاد هذه المشكلات، بل أنها أصبحت تتيح مكينة اتخاذ القرارات في كافة المجالات تقريبا.

وتم تقدير تعريفات المعلومات حتى الآن بـــ 400 تعريف وسوف نحاول توضيح مجموعة من هذه التعريفات كما يأتي:(4)

*مفهوم المعلومة لغة: المعلومات من حيث مدلولها اللغوي مشتقة من المادة اللغوية 'علم' وهي مادة غنية بالكثير من المعاني كالعلم والإحاطة بباطن الأمور والوعي والإدراك واليقين والإرشاد والإعلام والشهرة، والتميز والتيسير، وتحديد المعالم، والمعرفة، والتعليم والتعلم، والدراية .... إلى آخر ذلك من المعاني المتصلة بوظائف العقل وترجع كذلك إلى كلمة

'معْلَم' أي الأثر الذي يستدل به على الطريق وInformation هي المقابل الانجليزي لكلمة معلومات، وهذه الكلمة الانجليزية مشتقة من اللاتينية information والتي كانت تعني في الأصل الاتصال والتلقي.[5]

*مفهوم المعلومات اصطلاحا: فقد عرفت المعلومات وفقا للمعجم الموسوعي لمصطلحات المكتبات والمعلومات أنها البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاد القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها، أو تفسيرها، أو تجميعها في شكل ذي معنى والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وفي أي شكل". وعرفت المعلومات كذلك على أنها المقومات الجوهرية في أي نظام للتحكم

المشرع الأمريكي عرف المعلومات في قانون المعاملات التجارية الالكترونية لسنة 1999 بالفقرة العاشرة من المادة الثانية بأنها تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك.(6)

والمعلومات: هي الحقائق الثابتة التي يتم جمعاه والحصول عليها من أشخاص أو وثائق أو سجلات.

والمعلومات هي البيانات المرتبطة والواضحة بعد معالجتاه بالحاسب الآلي لتعبر عن معاني مفيدة.

***الأمن المعلوماتي:** هو حماية جميع أنواع المعلومات ومصادر الأدوات التي تتعامل معها وتعالجها، من منظمة وغرف تشغيل أجهزة، والأجهزة ووسائط التخزين والأفراد من السرقة أو التزوير أو التلف أو الضياع أو الاختراق وذلك باتباع إجراءات وقائية وضوابط واضحة[7].

***يعرف الامن المعلوماتي في هذه الدراسة:** بأنه اتخاذ إجراءات محكمة من أجل حماية فائقة ووقائية شاملة لمهددات المعلومة أو مواقع حفظها.

ج- الاختراق: تفتقد الكثير من المنظمات على الوعي الأمني، ولا تتخذ أية إجراءات أمنية لحماية معلوماتها، فلا توجد ميزانية مخصصة لأمن المعلومات ولا يوجد إجراءات خاصة بالتصرف عند حدوث الاختراق لوا يوجد أي برامج تدريبية وقائية أو للتدريب على كيفية التصرف في حالة حدوث الاختراق.

ويعرف الاختراق على أنه عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر وتصريحات الدخول بهدف الاطلاع على المعلومات، أو تخريبها أو سرقتها[8].

5: موضوع الجريمة المعلوماتية: يختلف موضوع الجريمة المعلوماتية بحسب اختلاف الزاوية التي ينظر فيها إزاء الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي، فمن ناحية قد يكون هذا الأخير نفسه موضوع للجريمة المعلوماتية ومن ناحية قد يكون النظام المعلوماتي هو وسيلة للجريمة المعلوماتية وأداة تنفيذها.

أ ــ الحالة الأولى: تتحقق هذه الحالة إذا كانت المكونات المادية للحاسب من معدات وكابلات وشبكات ربط وآلات طباعة هي محل أو موضوعا الجريمة وبالتالي لا تثير هذه الحالات مشكلة باعتبار أن هذه المكونات المادية محل الاعتداء تتمتع بالحماية القانونية.

ب ــ الحالة الثانية: تتحقق هذه الحالة عندما تكون مكونات الحاسب المعلوماتية غير المادية مثل البرامج المستخدمة والبيانات والمعطيات المخزنة في ذاكرة

الحاسب محلا أو موضعا للجريمة، ونظرا للطابع الخاص الذي يميز هذه المكونات فإنها لا تخضع لقانون العقوبات التقليدي

ج- الحالة الثالثة: في هذه الحالة لا يكون الحاسب محلا أو موضعا للجريمة وبالتالي لا يكون محلا للحماية الجنائية، ولكن تقع الجريمة بواسطته، فما هو إلا وسيلة لارتكابها، وحلها يختلف بحسب الشيء الذي ينصب عليه سلوك الفاعل والذي يشكل محل الحق أو المصلحة المحمية [(9)].

وعليه فإن موضوع الجريمة المعلوماتية هو المال المعلوماتي تمييزا لماليته المغايرة للمال التقليدي، والمال المعلوماتي هو الحاسب بكل مكوناته.

6: أسباب انتشار الإجرام المعلوماتي: يختلف مرتكبو جرائم المعلوماتية عن مرتكبي الجرائم الاعتيادية من حيث المبدأ وطريقة القيام بالعمل الجرمي، لكن بالنهاية يبقى الطرفان مخالفين للقانون، لذا يستحقوا العقاب بما اقترفوا من جرائم.

وإذا كانت الأنماط المختلفة للمجرم المعلوماتي تكشف عن انتشار هؤلاء المجرمين عند ارتكابهم الجريمة المعلوماتية في غرض واحد هو مجرد الهواية واللهو نتيجة انبهارهم بثورة المعلومات ثم من ناحية أخرى قد يكون الهدف هو تحقيق الثراء السريع أو إحدى الأسباب الشخصية.

ونحصر الأسباب التي تدفع لارتكاب الجرائم المعلوماتية في الآتي:

أ: الانبهار بالتقنية المعلوماتية: مع ظهور التقنية المعلوماتية وانتشارها في المجتمعات الحديثة سواء تعلق الأمر بالمعلومات أو الحواسب، فإن الأمر في النهاية يؤدي إلى انبهار المجرمين بهذه التقنية الحديثة، لذلك فإن هؤلاء ليسوا على جانب كبير من الخطورة، وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوفر لديهم أية نوايا سيئة، ونعطي مثلا على ذلك ما نشر في مجلة Expresse الفرنسية في شتنبر 1983 قصة بعنوان "ميلاد نزعة"[10] وتدور أحداث هذه القصة في أن عامل طلاء مباني قد توجه إلى أحد البنوك لإيداع شيك خاص به وتعاصر ذلك لحظة فصل الموزع الآلي للنقود حيث شاهد مستخدم صيانة الأجهزة الآلية

وهو يقوم باستخراج النقود من الآلة، عند الطلب عن طريق استخدام بطاقة خاصة وقد أحدث هذا الابتكار للآلة تصدعا في الحياة العادية لعامل الطلاء وقد حرص هذا الأخير على التدريب على تقنية الحاسوب لمدة عامين، ثم قام بالسطو على صانع الموزعات الآلية، وقد تمكن هذا العامل بفضل الآلة المسروقة من التوصل إلى أسلوب مطالعة السحب وألقي القبض عليه قبل أن يستفيد من نزعته المستحدثة.**(11)**

ب ــ الرغبة في تحقيق الثراء السريع: قد تدفع الحاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، ولذلك تتعدد الأساليب اللازمة للوصول إلى هذا الهدف المنشود، ولذلك فإن هذا السبب يعد من أكثر الأسباب التي تدفع إلى انتشار الإجرام المعلوماتي، تبرز الحاجة إلى تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة (مشاكل مالية، الديون، إدمان المخدرات...) مثال ذلك استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية[12] على اثنين وعشرين شريطا تحتوي على معلومات بخصوص عملاء إنتاج الشركة، وقد هدد السارق ببيعها للشركة المنافسة ما لم تدفع له فدية بمقدار 200000 دولار، وقامت الشركة بتحليل الموقف ففضلت الأداء مقابل استرداد الشرائط الممغنطة حيث أن قيمتها تفوق المبلغ المطلوب.

ج ــ الأسباب الشخصية: يعتبر محيط الانسان والبيئة التي يعيش فيها من العوامل المؤثرة في سلوكه وتصرفاته وغالباً ما تدفع مشاكل العمل إلى رغبة بالانتقام ووجود انظمة الكترونية تسهل له القيام برغباته فيعبث بمحتوياتها إلى درجة التخريب، أو يكون الدافع التحدي واثبات الجدارة أمام الآخرين بحيث يفتخر هذا الشخص بأن باستطاعته اختراق أي حاسوب أو أي نظام ولا يستطيع أحد الوقوف بوجهه**(13)**.

7- **خصائص الجريمة الإلكترونية:** تمتاز الجرائم المعلوماتية بعدة خصائص تميزها عن الجرائم التقليدية هي:

- **إمكانية ارتكاب هذه الجرائم عن بعد بمعنى أنها جريمة عابرة للحدود الوطنية:** فالعالم الآن أصبح قرية، يمكن التجول في أنحائها بمجرد الضغط على فأرة الحاسوب المرتبط بشبكة الانترنت، فيمكن لشخص ما أن يرتكب جريمة ما في دولة ما وتكون آثارها في دولة أو دول عديدة أخرى وهذا ما نسميه تلاشي الحدود بين الدول في العالم الافتراضي.

- عدم ترك هذه الجرائم لأي أثر خارجي بصورة مرئية ولهذا **يصعب إثباتها و**إن التحقيق في الجرائم المعلوماتية يتطلب الإلمام بتقنيات تكنولوجيات الإعلام والاتصال، وليس فقط تعلمها بل مواكبة التطور السريع الذي يحدث كل يوم في هذا المجال.

- هذه الجرائم لا عنف فيها، فلا جثث فيها ولا آثار دماء أو اقتحام من أي نوع بمعنى **أسلوب ارتكابها يجعل هذه** الجرائم المعلوماتية من الجرائم الهادئة التي لا تحتاج إلى عنف في ارتكابها.

- يتم اكتشاف معظمها بالصدفة البحثية **فصعوبة اكتشافها ونسبتها لشخص معين يجعل من هذه الجرائم** ترتكب بهدوء فإن اكتشافها يكون في كثير من الأحيان بمحض الصدفة

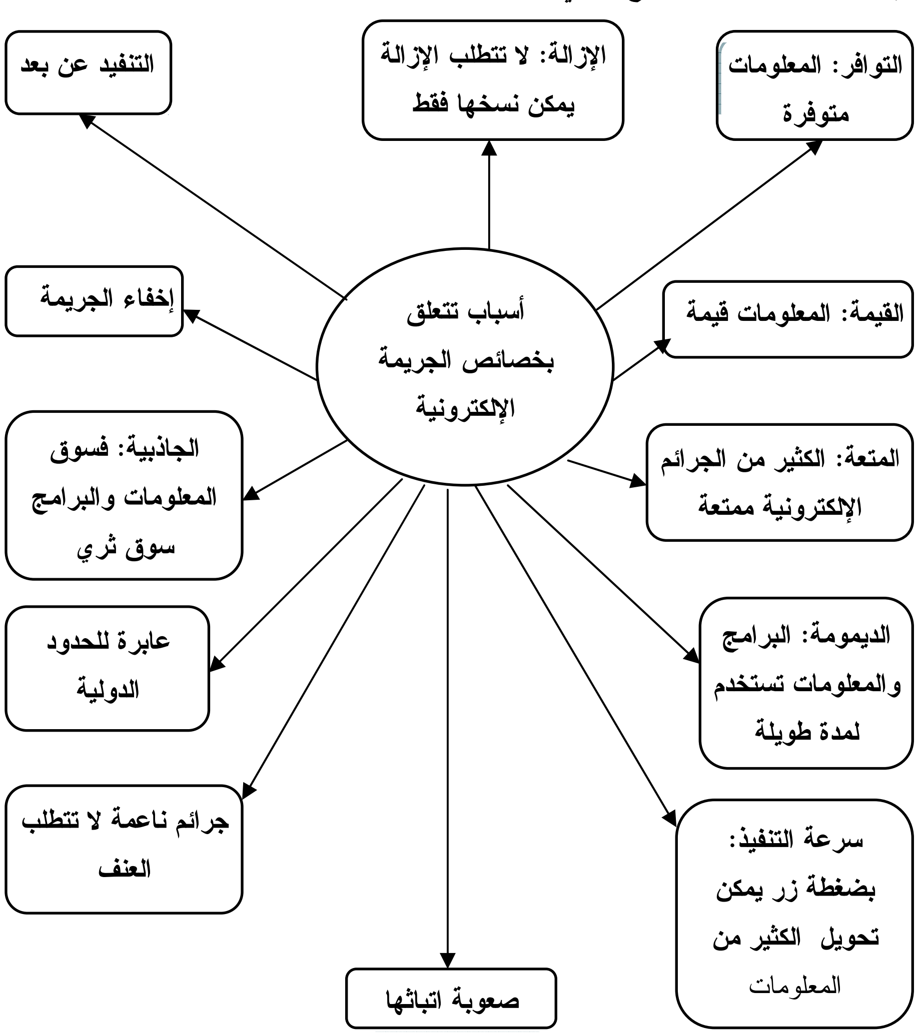
- ترتكب في الخفاء ولا يوجد لها أثر كتابي.

- قدرة الجاني على تدمير ما يعتبر دليل يمكن أن يستخدم لإدانته.

- **جريمة منظمة:** في البداية اعتبرت الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كسلسلة متتابعة من الاعتداءات على الشبكات، ولكنها تلونت بصبغة المافيا أي الجريمة المنظمة، منشئة بذلك "سوق سوداء" حقيقية للمعلومات المقرصنة، ابتداء من التعدي على حقوق الملكية الفكرية والفنية، والغش في البطاقات البنكية، فأصبحت.[14]

هناك صلات قوية بين الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التقليدية، وفي المقابل أصبح مجرمو المعلوماتية أكثر تنظيما يوما بعد يوم.

*** ويمكن وضع تصنيف آخر بما يسمى بأسباب تتعلق بخصائص الجريمة الإلكترونية حسب النموذج الآتي**



شكل رقم 1: يمثل مجموعة من خصائص الجريمة الإلكترونية تؤدي إلى ارتكاب الجريمة الإلكترونية.

•الشكل من إعداد الباحث.

8- تصنيف مرتكبو الجرائم الإلكترونية:

أ- المثاليين (المراهقين): وعادة ما يكون غير مدربين ومهرة وهم الشباب الذين تتراوح أعمارهم بين (13-26) سنة والذين يسعون إلى الاعتراف الاجتماعي.

ب- الجشع - المدفوع (المجرمون المهنيون): هذا النوع من مجرمي الإنترنت خطير، هذه الفئة عادة ما تكون عديمة الضمير وهم على استعداد لارتكاب أي نوع من الجرائم طالما أنها تجلب لهم المال.

ت- الافتراضي - الإرهابيون: هم مجموعة الأحداث والأكثر خطورة والدافع الأساسي ليس المال فقط ولكن أيضا لهم قضية ما والتي يدافعون عنها.[15]

I.**المعالجة الميدانية للدراسة:** تهدف الدراسة في إطارها الميداني إلى التعرف على معززات الجريمة الالكترونية وواقع الأمن المعلوماتي وتعتبر هذه الدراسة من الدراسات الوصفية التي تقوم بوصف الظاهرة ورصد خصائصها، وتتمثل الإجراءات الميدانية فيما يلي:

1.**المنهج المستخدم:** إن اختيار المنهج لا يأتي من قبيل الصدفة أو الميل، أو رغبة الباحث لمنهج دون آخر، بل إن موضوع الدراسة وأهدافها اللذان يفرضان نوع المنهج المناسب، وهذا الاختيار الدقيق هو الذي يعطي مصداقية وموضوعية أكثر للنتائج المتوصل إليها، وبما أن الدراسة الحالية تتمحور حول معرفة دوافع الإجرام المعلوماتي ومحفزاته فإنها تنتمي إلى الدراسات الوصفية، والتي تقوم بوصف الظاهرة من خلال تحديد ظروفها وأبعادها، والانتهاء إلى وصف عملي ودقيق ومتكامل للظاهرة أو المشكلة التي تقوم على الحقائق المرتبطة.

ويعرف المنهج الوصفي بأنه "أسلوب من أساليب التحليل المركز على معلومات كافية ودقيقة عن الظاهرة أو موضوع محدد، من خلال فترة أو فترات زمنية

معلومة، وذلك من أجل الحصول على نتائج عملية ثم تفسيرها بطريقة موضوعية"[16]

2- أداة الدراسة: تعتبر الاستمارة أكثر الوسائل المستخدمة لجمع البيانات شيوعا، وتعرف بأنها مجموعة من الأسئلة الموجهة للمبحوثين بهدف الحصول على بيانات ومعلومات بخصوص الموضوع المراد دراسته.

وقد استخدم الباحث استمارة المقابلة كأداة مهمة تمكن من جمع البيانات الخاصة بالدراسة، وقد تضمنت على **(17)** سؤال، منها ما هو مغلق، مفتوح ونصف مغلق موزعة على ثلاث محاور كانت كالآتي:

المحور الأول: حول البيانات الشخصية.

المحور الثاني: حول معززات أو محفزات الجريمة الإلكترونية.

المحور الثالث: حول واقع الحماية.

3- مجتمع وعينة الدراسة: قام الباحث بتطبيق الدراسة ميدانيًا على عينة من مخترقي الإنترنت (الهاكرز) بعد ما واجهته العديد من الصعوبات في الحصول على عدد من المبحوثين، كون هذا الامر يتعلق بكشف أسرار تتميز بطابع الخفاء وقد تمت الدراسة وفق عينة كرة الثلج حيث تم الاتصال بأحد المخترقين الذي بدوره دلّنا على مخترق آخر وهكذا كان الحال بالنسبة للثالث والرابع حتى بلغنا **(20)** مبحوث. وهذا في فترة ما بين 2015/08/05 إلى غاية 2016/09/05 وفي نفس الفترة قمنا بالاتصال ببعض تقنيي الحماية من موقع sndl وغيره من المختصين في هذا المجال.

لقد تكونت عينة الدراسة من(40) فرد مقسمة بين مخترقين وتقنيي حماية في ولاية قسنطينة.

4- عرض وتحليل البيانات: وسيتم التطرق في هذا العنصر إلى عرض البيانات المتحصل عليها وتحليلها وتفسيرها وصولا للإجابة على التساؤل المركزي:

5 – تفريغ البيانات

1 – الجنس:

خاص بعينة المخترقين			خاص بتقنيي الحماية		
الجنس	التكرار	النسبة المئوية	الجنس	التكرار	النسبة المئوية
أنثى	02	**10%**	**أنثى**	**04**	**20%**
ذكر	18	**90%**	**ذكر**	**16**	**80%**
المجموع	20	**100**	**المجموع**	**20**	**100%**

2– السن:

خاص بعينة المخترقين			خاص بتقنيي الحماية		
السن	التكرار	النسبة المئوية	السن	التكرار	النسبة المئوية
أقل من عشرين سنة	03	**15%**	أقل من عشرين سنة	**02**	**10%**
من 20 إلى 30 سنة	10	**50%**	من 20 إلى 30 سنة	**07**	**35%**
أكثر من ثلاثين سنة	07	**35%**	أكثر من ثلاثين سنة	**11**	**55%**
المجموع	20	**100**	**المجموع**	**20**	**100%**

3 ـ الحالة الاجتماعية:

خاص بعينة المخترقين			خاص بتقنيي الحماية		
الحالة الاجتماعية	التكرار	النسبة المئوية	الحالة الاجتماعية	التكرار	النسبة المئوية
أعزب	15	**75%**	أعزب	**07**	**35%**

متزوج	05	25%	متزوج	13	65%
المجموع	20	100	**المجموع**	20	100%

4- المستوى التعليمي:

خاص بعينة المخترقين			خاص بتقنيي الحماية		
المستوى التعليمي	التكرار	النسبة المئوية	المستوى التعليمي	التكرار	النسبة المئوية
أمي	00	00	أمي	00	00
ابتدائي	00	00%	ابتدائي	00	00
متوسط	03	15%	متوسط	00	00%
ثانوي	06	30%	ثانوي	02	10%
جامعي	08	40%	جامعي	13	65%
دراسات عليا	02	10%	أكثر من ثلاثين سنة	05	25%
المجموع	20	100	**المجموع**	20	100%

5- التخصص في مجال الإعلام الآلي:

خاص بعينة المخترقين			خاص بتقنيي الحماية		
الجنس	التكرار	النسبة المئوية	الجنس	التكرار	النسبة المئوية
نعم	12	%60	**نعم**	19	%95
لا	08	%40	**لا**	05	%05
المجموع	20	100	**المجموع**	20	100%

المحور الثاني: بيانات تتعلق بمعززات الجريمة الإلكترونية. **(**خاص بالمخترقين**)**

. 6 – غلاء برامج الحماية يعد محفز للجريمة الإلكترونية

الاحتمال	التكرار	النسبة
نعم	17	%85
لا	03	%15
المجموع	20	100

7. حب مساعدتك للآخرين يعد دافعا على الاختراق

الاحتمال	التكرار	النسبة
نعم	15	%75
لا	05	%25
المجموع	20	100

في حالة إجابتك بنعم في الجدول(7)	التكرار	النسبة
صعوبة الحصول على المادة العلمية	05	%25
الأثمان الباهضة للبرامج الحاسوبية والؤلفات التعليمية	15	%75

8. الجهل بالقوانين الردعية يعد محفزا للاختراق

الاحتمال	التكرار	النسبة
نعم	18	%90
لا	02	%10
المجموع	20	100

9. المنفعة المادية تعد محفزا للجريمة الإلكترونية

الاحتمال	التكرار	النسبة
نعم	16	%80
لا	04	%20
المجموع	20	100

10. الحقد وحب الانتقام وعامل التحدي يعد دافع للاختراق

الاحتمال	التكرار	النسبة
نعم	12	%60
لا	10	%40
المجموع	20	%100

المحور الثالث: بيانات تتعلق بواقع الأمن المعلوماتي:

11. ضعف برامج الحماية يعد مهدد للأمن المعلوماتي

الاحتمال	التكرار	النسبة
نعم	20	%100
لا	00	%00
المجموع	20	%100

12. قوة النظام القانوني تحد من الجريمة الإلكترونية

الاحتمال	التكرار	النسبة
نعم	16	%80
لا	04	%20
المجموع	20	%100

13. غلاء البرامج والمؤلفات العلمية (كتب، مجلات...) مهدد لأمن المعلومات

الاحتمال	التكرار	النسبة
نعم	17	%85
لا	03	%15
المجموع	20	%100

14- ضعف الحماية لقواعد البيانات يعتبر أساس في الإجرام المعلوماتي

الاحتمال	التكرار	النسبة
نعم	19	%95
لا	01	%05
المجموع	20	%100

15- الصراعات الدولية والإقليمية تعد سبب في تهديد الأمن المعلوماتي

الاحتمال	التكرار	النسبة
نعم	17	%85
لا	03	%15
المجموع	20	%100

16-الوعي والثقافة الإلكترونية يحد من تهديد الأمن المعلوماتي

الاحتمال	التكرار	النسبة
نعم	15	%75
لا	05	%25
المجموع	20	%100

6- تحليل النتائج: بعد تفريغ بيانات استمارة المقابلة، وتزامنا مع التحليل الكمي للنتائج، تبين لنا أن نسبة المخترقين (الهاكرز) أو المجرمين الإلكترونيين الذكور أعلى بكثير من نسبة الإناث وهذا راجع إلى الثقافة السائدة لذى الذكور

كون هذه الظاهرة فيها جزئ من التحدي والرجولة ولهذا بلغت نسبة الذكور المجرمين إلكترونيا 90 بالمئة، وقد سجلت نسبة المجرمين الإلكترونيين في عمر بين 20 سنة وسنة30 نسبة 50 بالمئة في حين أن نسبة التقنيين في هذا السن بلغت نسبتهم 35 بالمئة هذا يعني أن المخترقين أعمارهم في سن الشباب، وأن نسبة تقنيي الحماية في سن أكثر من 30 سنة وهذا راجع لمتطلبات هذا المجال الذي يركز على الخبرة، كما أنه سجلت نسبة 15 بالمئة بالنسبة للمخترقين في السن الأقل من عشرين سنة أي مراهقين، وكما هو معلوم أنه هناك فئة من الهواة من المراهقين يحبون اللهو وحب الاطلاع على هذا المجال، أما فيما يخص تقنيي الحماية فتعتبر نسبة الذكور هي الأخرى عالية وهذا راجع لمثل هذه التخصصات المرغوب فيها عند الذكور أكثر من الإناث وذليل ذلك سجلت نسبة 60 بالمئة للمتخصصين في الإعلام الآلي من المخترقين ونسبة 95 بالمئة لتقنيي الحماية ممن درسوا تخصصات في الإعلام الآلي، وما تجدر الإشارة إليه هنا هو أن نسبة 40 بالمئة من المجرمين الالكترونيين لم يدرسوا تخصصات في الإعلام الآلي وإنما تعلموه وفق اجتهادهم الخاص، أما فيما يخص الحالة الاجتماعية فنجد المجرمين الإلكترونيين معظمهم عزاب حيث سجلت نسبة 75 بالمئة في حين أن نسبة تقنيي الحماية المتزوجين عالية أي 65 بالمئة وهذا راجع لطبيعة عمل تقنيي الحماية التي تتطلب خبرة كبيرة، أما من حيث المستوى التعليمي سجلت نسبة 40 بالمئة بالنسبة للمخترقين الجامعيين في حين نسبة تقنيي الحماية الجامعيين كانت 65 بالمئة كون هذا التخصص يتطلب علم واسع بالإعلام الآلي في حين نجد أن نسبة المجرمين الالكترونيين الذين أنهو تعليمهم في المرحلة الثانوية مرتفعة نوعا ما تصل 30 بالمئة في حين تنخفض عند التقنيين إلى عشرة بالمئة وهذا راجع كما قلنا سابقا لنوعية التخصص، وتأتي نسبة تعتبر عالية بالنسبة للمجرمين الإلكترونيين الذين أنهو دراستهم في المتوسط، وهذا راجع لحب التحدي وحب الاطلاع وإثبات الذات عند الهاكرز حيث يجدون متعة في ذلك وإثبات للذات

خاصة بالنسبة للمراهقين الأقل من عشرين سنة، في حين أن النسبة تنعدم بالنسبة للتقنيين في هذا المرحلة التعليمية كما أن الجهل بالقوانين يعد سببا في انتشار ظاهرة الإجرام عند سن ما دون العشرين وعند الذين أنهو دراستهم في المتوسط أو الثانوي وهذا راجع لجهلهم بالقوانين الردعية للإجرام الإلكتروني، ولو نظرنا إلى نسبة الذين بلغوا الدراسات العليا نجدها عند المخترقين تنخفض وعند التقنيين ترتفع وهذا راجع للعلم بالقوانين ولبلوغ سن يخول لهم فهم الجريمة.

أما بالنسبة لمحور معززات الجريمة الإلكترونية نجد أن غلاء برامج الحماية يعد محفزا للجريمة الالكترونية إذ أن 85 بالمئة من عينة الدراسة أجابت بنعم، في حين أظهرت نسبة 75 بالمئة من مجتمع الدراسة، الخاص بالهاكرز أنهم يحبون مساعدة الآخرين وذلك بالاختراق ونشر المعلومات وتهديد الأمن المعلوماتي، مع المساعدة في كسر الحماية وتهديد الملكية الشخصية مستدلين بذلك بصعوبة الحصول على المادة العلمية، وبالتكاليف الباهظة للكتب والأبحاث العلمية وكذلك للبرامج أي بنسبة 75 بالمئة.

أما فيما يخص الجهل بالقوانين التي تردع الاختراق والإجرام الالكتروني تبين أنّ نسبة 90 بالمئة جاهلة بالقوانين، في حين أنّ مثل هذه الجرائم لا تزال مغيبة لحد اليوم وغير مشهورة في ثقافتنا والدليل على ذلك أنّ في الجدول 16 حول الثقافة الإلكترونية بيّن أن 75 بالمئة من مجتمع البحث يرون أن الوعي بالثقافة الإلكترونية يحد من تهديد الأمن الالكتروني، وقد سجلت نسبة 80 بالمئة من المبحوثين الذين يرون أن المنفعة المادية التي يجنيها المخترق سبب في جريمته الإلكترونية وسبب في تهديده للأمن المعلوماتي، وهذا راجع لنسب الفقر ولغلاء المعيشة، ولغلاء البرامج والوسائل التعليمية.

قد سجلت نسبة 60 بالمئة إجابات بنعم في سؤال هل الحقد وحب الانتقام وعامل التحدي معزز للجريمة الإلكترونية، وهذا راجع للتركيبة الثقافية للمجتمعات العربية وخاصة الجزائرية في كون أن الهاكرز لهم حملات متوالية سواء على اليهود أو

على المغرب وكذلك يحركهم حب الاطلاع والتحدي ولأن معظمهم مراهقين وهذه هي صفة المراهقة والشباب.

وإذا انتقلنا إلى المحور الثالث الخاص بالبيانات التي تتعلق بواقع الأمن المعلوماتي فإننا نجد في السؤال الأول أن نسبة 100 بالمئة أجابت أن الحماية ضرورية وأن واقع الأمن المعلوماتي وما يهدده هو قلة الحماية أما فيما يخص إجابات السؤال الثاني فإن النظام القانوني يحد من تهديدات الجريمة الإلكترونية وذلك حسب الإجابات بنسبة 80 بالمئة.

أما إجابات السؤال الثالث في هذا المحور كانت كالآتي هو أن غلاء البرامج والكتب وغيرها يعد مهدد للأمن المعلوماتي بنسبة 85 بالمئة، وهذا ما يسبب الاختراق وحب نشر العلم والوثائق للفقراء والمحتاجين والباحثين تضامنا معهم.

قد بينت نسبة 95 بالمئة أن ضعف الحماية سبب في الإجرام الإلكتروني، هذا بالنسبة لقواعد البيانات، وأنه لا توجد مراقبة في عملية نسخ ولصق المعلومات أو طباعتها خاصة في قواعد البيانات الخاصة بالأبحاث العلمية.

وإذا نظرنا إلى الزمن الحالي وجدنا أن الصراعات السياسية والإقليمية أصبحت تحرك جيوش من الهاكرز قصد تدمير بيانات دول ونشرها مثل ما حدث مع جماعة الأنينيموس في السنوات الأخيرة وهجماتها على اليهود وقد طرحنا سؤال في ذلك فكانت إجابات 85 بالمئة بنعم أي عامل تهديد لأمن المعلومات

كما بين أيضا الكثير من عينة البحث أن الوعي والثقافة الإلكترونية تحد من تهديد الأمن المعلوماتي بنسبة 75 بالمئة وما نعاني منه اليوم هو نابع عن الجهل بالحماية وبالثقافة الإلكترونية ولهذا نكون عرضة للتخريب.

وللإجابة عن التساؤلات المطروحة نجد:

معززات الجريمة الإلكترونية كانت كالآتي: غلاء برامج الحماية يعد محفز للجريمة الإلكترونية وكذلك حب مساعدتك الآخرين يعد دافعا على الاختراق والإجرام الإلكتروني، نظرا للجهل بالقوانين الردعية، في ظل البحث عن المنفعة

المادية التي تعد محفزا قويا على الإجرام الإلكتروني مع عامل الحقد وحب الانتقام وعامل التحدي وحل إظهار الذات.

واقع الأمن المعلوماتي كان كالآتي: من مهددات الأمن المعلوماتي وكما تبين ضعف برامج الحماية يعد مهدد للأمن المعلوماتي وكذلك عدم احتواء النظام القانوني للجرائم الإلكترونية، وعدم حصرها، كما تلعب كذلك مؤشرات غلاء البرامج والمؤلفات العلمية (كتب، مجلات ...) دورا كبيرا في تهديد أمن المعلومات في ظل ضعف الحماية لقواعد البيانات، مع الصراعات الدولية والإقليمية التي تفرض عدم تطبيق القوانين الدولية والإقليمية وعدم التكاثف حول تطبيق القوانين وسن نظم حماية موحدة ويبقى أكبر مؤشر كما نراه يبرز واقع الأمن المعلوماتي هو الوعي والثقافة الإلكترونية والذي في نفس الوقت عامل يحد من تهديد الأمن المعلوماتي بشكل كبير وقوي.

الخاتمة:

لقد سعت هذه الدراسة إلى توضيح جانب مهم من معززات الجريمة الالكترونية، وقد خلصت إلى أن الجزائر تعاني من ضعف في حماية قواعدها نظرا للتكلفة الباهظة لبرامج الحماية، كما أن الثقافة السائدة تلعب دور في تفشي مثل هذه الجرائم وكذلك الجهل بقانون العقوبات لمثل هذه الجرائم التي تعد في عالم افتراضي، صعب مراقبتها وصعب متابعتها.

ولقد أصبح من الواجب بذل جهود من أجل تطوير قواعد بيانات محمية، وسن نصوص وجرد عقوبات تحمي الحقوق الشخصية والملكية الخاصة.

ونخلص في هذه الورقة البحثية إلى أن الجريمة المعلوماتية، من أكبر التحديات التي نواجهها في عالمنا المعاصر، إن لم تكن أكبرها على الإطلاق، وعلى الدولة أن تعمل على الحد من مثل هذه الجرائم بتكوين أجهزة متابعة وقواعد معلومات محمية وفرق متخصصة فنياً، في التقنية المعلوماتية، ويجب أن تسعى الجزائر إلى تطوير تكنولوجيا معلوماتها بمعنى أن تبتعد عن الاستيراد لمثل هذه التكنولوجيا

بدون حماية كافية كما يجب عليها أن تضع تخصصات في الجامعات مواكبة للتطور التقني.

والملاحظ أن مشرعنا قد استدرك مؤخرا الفراغ القانوني الملحوظ في مجال الاجرام المعلوماتي وقد اعتمد في ذلك حلا يضمن حماية مزدوجة للحاسب الآلي من خلال نصوص حق المؤلف من جهة، ومن خلال نصوص خاصة أدمجها في قانون العقوبات من جهة أخرى ولكن أين هي الثقافة والمعرفة القانونية لذا العامة بل حتى الخاصة من المتعلمين.

ومن بين التوصيات التي نسطرها:

- العمل على عقد المزيد من الندوات العلمية والمؤتمرات حول العلاقة بين المعلوماتية والجريمة المعلوماتية.
- على الدول العربية المضي في عقد اتفاقات دولية إقليمية وعربية للتعاون على مكافحة الجرائم المعلوماتية مع ضرورة التعاون الدولي لمواجهة صور السلوك ا لمنحرف في البيئة المعلوماتية وهذا ما أوحت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة في سنة2001 وذلك بتشجيع الدول على إدراج الجرائم المعلوماتية في قوانينها العقابية.
- وضع تخصصات سواء في الاعلام الآلي وتكنولوجيا الاتصال، أو في الإدارة والقانون تهتم بمجالات الإعلام والتقنية والنظم ومجالات الحماية وضبط الجرائم وغيرها.
- السمة المميزة للكثير من الجرائم المعلوماتية هي أنها من النوع العابر للحدود TRANSNATIONAL. وبالتالي فإنه بات من الضروري إبرام معاهدات للتسليم أو للمعاينة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي وإن وجدت فإنها غير كافية لمواجهة المتطلبات الخاصة.

وتبقى الجريمة المعلوماتية كما يقول الدكتور محمود صالح العادلي في روقة عمل مقدمة في جرائم المعلومات ماهيتها وصورها:

الجريمة المعلوماتية هي:

الابن غير الشرعي.........

الذي جاء نتيجة للتزاوج بين......

ثورة تكنولوجيا المعلومات..........

مع العولمة.

أو هي:

المارد ...... الذي خرج من القمقم.........

ولا تستطيع العولمة أن تصرفه..............

بعد أن أحضرته .... الممارسة السيئة لثورة تكنولوجيا المعلومات......

الملاحق :

ضع علامة (x) في المكان المناسب

المحور الأول: البيانات الأولية

1- الجنس:

✓ ذكر ☐ أنثى ☐

2- السن :

✓ أقل من عشرين سنة ☐ من 20 إلى 30 سنة ☐

✓ أكثر من 30 سنة ☐

3- الحالة الاجتماعية:

✓ أعزب ☐ متزوج ☐

4- المستوى التعليمي:

✓ أمي ☐ ابتدائي ☐ متوسط ☐ ثانوي ☐

✓جامعي ☐ دراسات عليا ☐

5- هل تخصصك الدراسي في مجال الإعلام الآلي:

نعم ☐ لا ☐

المحور الثاني: بيانات تتعلق بمعززات الجريمة الالكترونية

6- هل ضعف الحماية دافع للاختراق ؟ :

نعم ☐ لا ☐

7- هل حب مساعدتك للآخرين يعد دافعا للجريمة الإلكترونية ؟

نعم ☐ لا ☐

إذا كانت الإجابة ب "نعم"، لماذا ؟

✓ صعوبة الحصول على المادة العلمية. ☐

✓الأثمان الباهضة للبرامج الحاسوبية والؤلفات التعليمية. ☐

✓أخرى تذكر:.......................

8- هل الجهل بالقوانين الردعية يعد محفزا للاختراق؟

✓ نعم ☐ لا ☐

9- هل المنفعة المادية تعد محفزا للجريمة الالكترونية ؟

10-هل الحقد وحب الانتقام ودافع التحدي يعد دافع للاختراق

نعم ☐ لا ☐

11 - إن كانت هناك دوافع أخرى للاختراق أذكراها

....

المحور الثالث: بيانات تتعلق بواقع الامن المعلوماتي :

12- هل ضعف برامج الحماية يعد مهدد للأمن المعلوماتي؟

✓ نعم ☐ لا ☐

13- هل قوة النظام القانوني تحد من الجريمة الالكترونية؟

✓ نعم ☐ لا ☐

14- هل غلاء البرامج والمؤلفات العلمية (كتب، مجلات ...) مهدد لأمن المعلومات؟

نعم ☐ لا ☐

15- هل ضعف الحماية لقواعد البيانات يعتبر أساس في الإجرام المعلوماتي

نعم ☐ لا ☐

16- هل الصراعات الدولية والإقليمية تعد سبب في تهديد الأمن المعلوماتي

نعم ☐ لا ☐

17 - هل الوعي والثقافة الالكترونية يحد من تهديد الاختراق

نعم ☐ لا ☐

18- كيف ترى واقع الامن المعلوماتي في الجزائر ؟

....

شكرا لتعاونكم معنا.. آراؤكم ومقترحاتكم تهمّنا

قائمة المصادر والمراجع:

1- وليد محمد حجاج شرح قانون العقوبات القسم العام كلية الحقوق جامعة أسيوط 2006.

2- محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004. ص: 43.

3- سامي علي حامد عياذ، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي الإسكندرية، 2007.

4- رصاع فتيحة: الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة ماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان، الجزائر 2012/2011 ص 24-25.

5- رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكات الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص10.

6- رصاع فتيحة: الحماية الجنائية للمعلومات على شبكة الانترنت: مرجع سابق، ص 26.

7- م منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها: رسالة ماجستير، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية السعودية ص 09، 2008.

8- منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها رسالة ماجستير، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية السعودية ص 34، 2008.

9- قارة أمل، الجريمة المعلوماتية، رسالة ماجستير، في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، الجزائر، ص 21.

10- محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات دار الثقافة للطباعة والنشر 1987، ص: 48.

11- المرجع نفسه. ص: 48.

12- محمد علي العريان: الجرائم المعلوماتية – دار الجامعة الجديدة للطباعة والنشر، ط 2004، ص: 66.

13- http://kenanaonline.com/users/internet-safety/posts/143404. يوم 2015/0/18

14- قارة أمل، الجريمة المعلوماتية، رسالة ماجستير، في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، الجزائر، ص 25 بتصرف.

15- ذياب موسى البداينة: الجرائم الإلكترونية المفهوم والأسباب، ورقة بحثية مقدمة للملتقى العلمي: الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، ص 21، 2014.

16- غازي عناية، منهجية إعداد البحث العلمي، دار المناهج، عمان الأردن 2008 ص77.

الهوامش:

1- وليد محمد حجاج شرح قانون العقوبات القسم العام كلية الحقوق جامعة أسيوط 2006.

2- محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004. ص: 43.

3- سامي علي حامد عياذ، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي الإسكندرية 2007، ص 38 .39. 40.

4 – رصاع فتيحة: الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة ماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان، الجزائر 2012/2011، ص 24-25.

5 – رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكات الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص 10.

6 – رصاع فتيحة: الحماية الجنائية للمعلومات على شبكة الانترنت: مرجع سابق، ص 26.

7- منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها: رسالة ماجستير، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية السعودية، ص 09، 2008.

8- منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة ماجستير، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية السعودية، ص 34، 2008.

9- قارة أمل، الجريمة المعلوماتية، رسالة ماجستير، في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، الجزائر، ص 21.

10- محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات، دار الثقافة للطباعة والنشر 1987، ص: 48.

11- المرجع نفسه. ص: 48.

12- محمد علي العريان: الجرائم المعلوماتية – دار الجامعة الجديدة للطباعة والنشر، ص: 66.

13- http://kenanaonline.com/users/internet-safety/posts/143404

14- قارة أمل، الجريمة المعلوماتية، رسالة ماجستير، في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، الجزائر، ص 25 بتصرف.

15- ذياب موسى البداينة: الجرائم الإلكترونية المفهوم والأسباب، ورقة بحثية مقدمة للملتقى العلمي: الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، ص 21، 2014 .

16- غازي عناية، منهجية إعداد البحث العلمي، دار المناهج، عمان الأردن، 2008. ص77.

حق حيازة الفكرة العلمية وأفق شيوع المعرفة بين الالتزامات الأخلاقية والمطالبات القانونية.

أ. عبد الحفيظ شريف

جامعة محمد البشير الإبراهيمي، برج بوعريريج.

ملخَّص: تتناول المداخلة مقاربة بين المطالبة الفرديَّة لمنتجي الأفكار والمعارف بحقِّ حماية نتاجهم الفكريِّ من السَّطو والاعتداء من منطلق أنَّه مكسب ذاتيٌّ وخصوصيَّة فرديَّة من جهة، وبين مشروعيَّة شيوع المعرفة وواجب اشتراك الإنسانية في خدمة العلوم والمعارف وترقيتها على أنَّ ذلك مصلحة جماعية وخدمة عامَّة من جهة أخرى، لتحاول في الأخير الوقوف على ما يمكن أنْ يَسُدَّ الفجوة بين المطْلَبَيْن، محاولة متابعة هذه الجدلية من وجهة نظر ذات أبعادٍ ثلاثة: الأخلاقية في الممارسة والقانونية في الحيازة، والخدمة العلميَّة في الغرض.

مقدمة: شكّل التقارض المعرفي البشري بفعل التَّجاور والاحتكاك مظهرا ساد كل التَّجمُّعات الإنسانيَّة عبر التَّاريخ، وأخذ أشكالا بسيطة حينا ومعقَّدة حينا آخر، مسايرا نمط حياة تلك المجتمعات في بساطتها وتعقيدها، ومع ارتقاء الإنسان الفكريِّ، واستواء أنماط نتاجه المعرفيِّ، برزت مسألة نسبة الآراء والمنجزات العلميَّة والأدبيَّة لأصحابها، وحقِّ حيازة آثارها، لا يختلف الأمر في ذلك عن حقِّ امتلاكهم لمتاعهم وأموالهم، بل ربّما أكثر من ذلك، فمن الآراء والأفكار والتَّصانيف ما لا يُقدَّر بثمن.

وبفعل جاذبيَّة هذا النَّوع من الإنجازات، والرَّغبة في تحصيل قيمتها المادِّيَّة والمعنويَّة؛ باتت محلَّ نزاع مستمرٍّ، طالما ثار حوله جدلُ الانتساب وحقُّ التَّملُّك، وكان من نتائج ذلك الصِّراع أنِ استفاد البعضُ بثمرات أعمال أدرّت

عليهم أموالا وشهرة، وغُمِط أصحابُ الحقوق حقوقَهم بعد أنِ اعتُدِيَ عليهم في نتاجهم الفكريّ أو الأدبيِّ أو العلمي بسبب أو بآخر.

ومقابل مشروعيَّة تملُّك المبدعين لهذا النَّوع من النِّتاج، ووجوب حمايتهم من الاعتداء والسَّطو بنسبته أو نسبة بعضه إلى غيرهم؛ تقف ضرورة إشاعة هذا النِّتاج واستفادة المجموعة البشريَّة منه – وهو ما يُكسِبُه قيمته الحقيقيَّة– لنجد أنفسنا أمام تعالُقٍ جدليٍّ يقوم أحدُ طرفَيْه على أحقِّيَّة مطالبة الفرد بمشروعيَّة التَّملُّك لما أَبْدع وألّف، ويرتفع طرفه الآخر على مسلَّمة شيُوع المعارف والعلوم بين المجموعة البشريَّة، فما الحدود الفاصلة بين الطرفين؟ وما المعالم الّتي يمكن الاهتداء بها في ضبط حقِّ كلِّ طرفٍ والتزامه؟

تلك هي القضية الّتي ستعرض لها هذه الورقة من زوايا ثلاث.

1- **الأخلاقيّة:** وتتابع فيه الالتزام الذّاتي بما أقرته الشَّرائع واللَّوائح والاتِّفاقيات، بل والأعراف الإنسانية.

2- **القانونية:** وتعرض فيه للوجهة القانونيَّة العامَّة الّتي تؤطر العلاقة الدَّقيقة بين المؤلِّفين والمبدعين والمتلقِّين عنهم.

3- **العلميَّة:** وتتناول فيه نموذجين تاريخيَيْن كبيرَيْن من المعالجة العلميَّة للبحث والاستفادة، وطرائق الإسهام في بناء التَّراكم العلمي الإنسانيّ.

الاكتساب المعرفي بين المنفعة والأخلاق: يبدو التَّوفيق بين الرَّغبة المادّية للمستفيدين من العلوم والمعارف، والالتزام الأخلاقيِّ بالطَّرائق التي تؤطر تحصيل هذه الاستفادات صعبا في مواضع كثيرة، إذ تحت ضغط الحاجة والرَّغبة في تحقيق أفضل الآمال، يجد الباحثون أنفسهم وسط تجاذُبات الطَّمع في بلوغ درجة علميَّة، أو استفادة معنويَّة أو مادِّيَّة، أو الظَّفر بمنصب إداريٍّ من جهة، وبين واجب الالتزام الأخلاقي بتحقيق تلك الأهداف المشروعة بطرق مشروعة، في الاشتمال بالحرص وركوب الصَّبر والاستعداد للتَّضحية، وفي كنف صراع هذه الثنائية ينبثق نموذجان:

أحدهما: صورة نموذجيَّة للخلق العلميِّ بحثا وإسنادا، يسعى الباحث فيه لتكوين نفسه، ويُضحِّي في سبيل ذلك بالكثير من جهده ووقته وماله، ويأبى على نفسه الاقتيات على موائد الآخرين، ويأنف من العيش على فُتاتهم، فهو بهذا الالتزام قد أحسن تمثيل العلم، وتشرَّف بالانتساب إلى أهله.

وثانيها: صورة نموذجية أيضا، ولكنّها في الرَّداءة حين يقبر بعض أشباه الباحثين خلقه ويشنق ضميره، فيستسهل الصَّعب، ويختصر الطريق الصَّعب الطَّويل بالإغارة والسَّلب والنَّهب، ويغنم من الوقت الثَّمين الكثير بالنَّسخ الغبيّ والنّقل الفاضح، وما هي إلاّ فترة حتّى تنتشر آثار صغر نفسه، فكم تحوّلت جلسات مناقشات الرَّسائل والأطروحات إلى جلسات لمحاكمات فاضحة، وكم تحوّل الأمل في بلوغ درجة علميَّة أو نيل منصب إداريٍّ بنشر مقال أو مُنجَز علمي إلى إدانة ثقيلة تلازم صاحبها أبدا، ومن تعجَّل الشَّيءَ قبل أوانه عُوقِب بحرمانه.

1- الموقف الشَّرعي من اغتصاب العلوم والمعارف: يشيع في الوسط العلمي تصنيف الاغتصاب (غير العلمي) للمعارف والأفكار تحت مسمَّى "السَّرقة" أو "الغش" أو "الخيانة" أو غيرها من المرادفات وهو فعل تمالأ النَّاس على التَّشنيع به وبفاعله، وتواترت نصوص التَّشريعات السَّماويَّة والوضعيَّة على استقباحه، وإيقاع أشكالٍ من العقوبات على فاعليه، وكثيرا ما يقابِل هذا الفعلَ الاستشهادُ بالنُّصوص الّتي تقبِّحُه، وتُشِيد بنقيضه، فتحضر نصوصٌ تُرغِّب في الأمانة، والصِّدق، والعفَّة، وهي نصوصٌ عامَّة، تُعَدُّ الأمانة العلميَّة أحد أعظم أنواعها، كما تحضر في المقابل نصوصٌ أخرى تُنفِّر من السَّرقة والخيانة والغشِّ والاحتيال، وهي أيضا نصوص عامَّة، ولا شكَّ أنَّ الغَصْب المعرفيَّ من أشنعها وأقبحها.

ولكنَّ أنسب الاستشهادات - في ما أعتقد- لهذه الظَّاهرة من القرآن الكريم هو ما جاء من قوله تعالى: ﴿ وَإِذۡ أَخَذَ ٱللَّهُ مِيثَٰقَ ٱلَّذِينَ أُوتُواْ ٱلۡكِتَٰبَ لَتُبَيِّنُنَّهُۥ لِلنَّاسِ

﴿ وَلَا تَكْتُمُونَهُۥ فَنَبَذُوهُ وَرَآءَ ظُهُورِهِمْ وَٱشْتَرَوْاْ بِهِۦ ثَمَنًا قَلِيلًا ۖ فَبِئْسَ مَا يَشْتَرُونَ ﴿١٨٧﴾ لَا تَحْسَبَنَّ ٱلَّذِينَ يَفْرَحُونَ بِمَآ أَتَوا۟ وَّيُحِبُّونَ أَن يُحْمَدُوا۟ بِمَا لَمْ يَفْعَلُوا۟ فَلَا تَحْسَبَنَّهُم بِمَفَازَةٍ مِّنَ ٱلْعَذَابِ ۖ وَلَهُمْ عَذَابٌ أَلِيمٌ ﴿١٨٨﴾ ﴾ [آل عمران: 187-188] فانطلاقا عن ملفوظ النَّص نلحظ التَّصريح بمفردات الظَّاهرة وعناصرها، واستعراض حالة أهلها ومآلهم، والإخبار عن النَّموذج التَّاريخيِّ الّذي خُصِّص بسبب النزول، إلاّ أنّ أَخْذَ أهل التَّفسير بمبدأ العبرة بعموم اللَّفظ لا بخصوص السَّبب يجعل من هذا النَّص أنموذجا كاملا في تعرُّضه لهذه الظَّاهرة وأفرادها، ويتجاوز الزَّمان والمكان.

جاء عن المفسِّرين في سبب نزول الآيتين أقوال على معهود قول أهل علوم القرآن بتعدُّد السَّبب والنَّازل واحد، وممَّا ورد في ذلك، ما ذكره ابنُ الجوزي قال: "وفي سبب نزولها ثمانية أقوال، أحدُها: أنَّ النبيّ ﷺ سأل اليهود عن شيء فكتموه، وأخبروه بغيره، وأرَوْه أنَّهم قد أخبروه به، واستحمدوا بذلك إليه وفرحوا بما أَتَوْا من كتمانهم إيَّاه، فنزلت هذه الآية، والثَّاني: أنَّها نزلت في قومٍ من اليهود، فرحوا بما يصيبون من الدُّنيا، **وأحبّوا أنْ يقول النَّاس: إنهم علماء** وهذا القول والذي قبله عن ابن عباس[1]. والآية الأولى صريحة في بيان موقع أهل العلوم عند الله، ومقدار المسؤولية التي حُمِّلوها أو تحمَّلوها ويكفي أن يكون عنوانها "ميثاقا" لم يستثن أحدا ممن انتسب إلى العلم، أيًّا كان دينه أو عرقه، أو زمانه أو مكانه، يقول الإمام عبد الرحمان الثَّعالبي (875هـ) "وقوله سبحانه: ﴿ وَإِذْ أَخَذَ ٱللَّهُ مِيثَٰقَ ٱلَّذِينَ أُوتُوا۟ ٱلْكِتَٰبَ ... ﴾ توبيخ لمعاصري النبيّ ﷺ ثمَّ هو مع ذلك خَبَرٌ عامٌّ لهم ولغيرهم، قال جمهورٌ من العلماء: الآية عامَّةٌ في كلِّ من علَّمه اللَّه عِلْماً، وعلماءُ هذه الأمَّة داخلُونَ في هذا الميثاقِ[2]". وإلى مثل قوله ذهب الإمام الرَّازي فقال: "اعْلَمْ أَنَّ ظَاهِرَ هَذِهِ الْآيَةِ وَإِنْ كَانَ مُخْتَصًّا بِالْيَهُودِ وَالنَّصَارَى فَإِنَّهُ لا يبعد أيضاً دخول المسلمين فيه[3]" وبأسلوب التَّعليل، وبيان وجه استلحاق كل من نسب إلى العلم بموعود الآية ووعيدها، من غير اقتصار

على من نزلت في شأنهم، يقول الشَّيخ الطَّاهر بن عاشور "وَهَذِهِ الآيَةُ وَإِنْ كَانَتْ فِي أَهْلِ الْكِتَابِ إِلَّا أَنَّ حُكْمَهَا يَشْمَلُ مَنْ يَرْتَكِبُ مِثْلَ صَنِيعِهِمْ مِنَ الْمُسْلِمِينَ لِاتِّحَادِ جِنْسِ الْحُكْمِ والعلّة فِيهِ[4]" فعلى قدر المقام الذي أولاه الله للعلماء من الخلق، فقد رتَّب على تقصيرهم وخيانتهم لميثاقهم معه وعيدا رهيبا يكافئ صنيعهم المستقبح، والآيتان بهذا تصوِّران وصفا إضافيًّا لقائمة طويلة من أوصاف هذه الطَّائفة (اليهود) التي نزل في شأنها هذا الأمر، حين أخذ الله العهد على علمائهم بأنْ يُبيِّنوا العلوم التي حواها كتابهم، وأنْ لا يكتموا ما فيها، فكان منهم الإعراض عمَّا نزل إليهم، بل واستبدلوه بأعراض رخيصة من الدنيا كالرِّشى وأشباهها، وليت الأمر توقَّف عند ذلك؛ بل تضاعف السخط بهم حين طلبوا المحمدة والثَّناء عند النَّاس على أفعال لم يفعلوها، ورغِبوا في الذِّكر الحسن مقابل ما هو في حقيقته جرائم وبوائق، وهذا وحده كافٍ لإنزالهم منازل الغضب والسخط والنظر إليهم بعين الذِّلة والاحتقار، يقول صاحب التَّحرير والتَّنوير: "وَهَذَا ضَرْبٌ آخَرُ جَاءَ بِهِ فَرِيقٌ آخَرُ مِنْ أَهْلِ الْكِتَابِ فَلِذَلِكَ عَبَّرَ عَنْهُمْ بِالْمَوْصُولِ لِلتَّوَصُّلِ إِلَى ذِكْرِ صِلَتِهِ الْعَجِيبَةِ مِنْ حَالِ مَنْ يَفْعَلُ الشَّرَّ وَالْخِسَّةَ، ثُمَّ لاَ يَقِفُ عِنْدَ حَدِّ الانْكِسَارِ لِمَا فَعَلَ، أَوْ تَطَلُّبِ السِّتْرِ عَلَى شَنْعَتِهِ، بَلْ يَرْتَقِي فَيَتَرَقَّبُ ثَنَاءَ النَّاسِ عَلَى سُوءِ صُنْعِهِ، وَيَتَطَلَّبُ الْمَحْمَدَةَ عَلَيْهِ[5]". وحتَّى يرتفع اللّبس الذي قد يُماري فيه هؤلاء وأمثالُهم في كلِّ ملَّة؛ جاء التَّصريح بعظم جرم الانتساب إلى أهل العلم تسلُّقا، والسَّعي إلى الظُّهور في مقام العلماء كذبا "قَالَ عِكْرِمَةُ: نَزَلَتْ فِي فِنْحَاصَ وَأَشْيَعَ وَغَيْرِهِمَا مِنَ الأَحْبَارِ يَفْرَحُونَ بإضلالهم النَّاس بنسبة النَّاسِ إِيَّاهُمْ إِلَى الْعِلْمِ **وَلَيْسُوا بأهل علم**[6]" وللتشنيع أكثر في حقِّ هؤلاء شَفَع بعض المفسِّرين وعيد القرآن بوصف ووعيد الحديث عن رسول الله ﷺ فيقول ابن كثير: وَقَوْلُهُ تَعَالَى ﴿ لَا تَحْسَبَنَّ ٱلَّذِينَ يَفْرَحُونَ بِمَآ أَتَواْ ﴾ الآيَةَ يَعْنِي بِذَلِكَ الْمُرَائِينَ الْمُتَكَثِّرِينَ بِمَا لَمْ يُعْطَوا، كَمَا جَاءَ فِي الصَّحِيحَيْنِ عَنْ رَسُولِ اللَّهِ ﷺ "مَنِ ادَّعَى دَعْوى كَاذِبَةً لِيَتَكَثَّر بِهَا لَمْ يَزِدْه اللَّهُ إِلاَّ قِلَّة[7]" وَفِي

الصَّحِيحِ: "الْمُتَشَبِّعُ بِمَا لَمْ يُعْطَ كَلَابِسِ ثَوْبَي زُور"[8][9] والنَّصان يصفان بدقَّة الدَّافع النَّفسي الذي يختفي وراءه المتكثِّرون بالعلم كذبا، والمُدَّعون للشَّبع بالمعارف والتَّضلُّع في المسائل والقضايا زورا، ولاستئصال هذا الداء، نبَّه النبي ﷺ من هذا حالُه إلى علاج من جنس الداء، وهو إلفات نظر هؤلاء إلى تصوُّر المآلات، والتفكُّر في العواقب، فأخبر أنَّ عاقبة التَّكثُّر بحقوق الآخرين قلَّة وذلَّة وأنَّ المنتسب إلى حوزة العلم والعلماء من غير طريقها كالذي يُقتاد للإدلاء بشهادة زور، قال أبو سعيد الضَّرير في شرح قوله: كلابس ثَوْبَيْ زُور، "هو أنْ يستعير شاهدُ الزُّور ثوبَيْن يتجمَّل بهما ويتحلَّى بهما عند الحاكم، وإنَّما يريد أنْ يُقيم شهادته. وقال بعض أهل المعرفة بلسان العرب: ولقوله: ثوبَيْ، التَّثنيَّة معنى صحيحٌ؛ لأنَّ كذب المتحلِّى بما لم يُعْطَ مُثنَّى، **فهو كاذبٌ على نفسه بما لم يأخذ، وكاذب على غيره بما لم يبذل**[10]". وهذه بالتفصيل حقيقة المغِيرِين على المعارف والعلوم بغير وجه صحيح، وهذه أوصافهم جاءت في بيان القرآن الكريم، وعلى لسان الموحى إليه من الخبير العليم.

لقد دأبت النُّصوص التَّشريعيَّة الإسلاميَّة في معالجة الظَّواهر الإنسانيَّة المشينة، على ربط المتلقِّي برقيب عليه من نفسه، وإحياء موات ضميره، وبعث روح الاستقامة والالتزام من داخله، فذلك أنجع في العلاج، وأضمن للنَّتائج وأكثر اقتصادا في الجهد والوقت والمال، وجعلت ذلك أصلا تستقطب به أكبر قدر ممكنٍ من الملتزمين ذاتيًّا، والمستقيمين سجيَّة، ثمَّ عمدت إلى التَّشريعات الرَّادعة التي تأخذ على أيدي العابثين والمستهترين، فشرَّعت لهم الحدود ومقادير الجزاء وأنواعها، وبالنَّظر إلى نوعية النُّصوص السَّابقة؛ نستطيع الوقوف على نوع من الرَّدع الواعظ، فهو أليق بأهل العلم لو كانوا يعلمون فإذا ما سمح هؤلاء لأنفسهم بالدُّون، ورضوا عوض الكرامة بالهُون، نزلت معهم النُّصوص فعامَلَتهُم كما تعامل صغار النفوس من سراق البيض وسقط المتاع

فيستحضر العلماء والمُفتُون للتَّشنيع على هؤلاء النُّصوص الكثيرة في تحريم السَّرقة والغشِّ والخيانة، ويبيِّنون الحقيقة الفقهية لمثل هذه الأفعال.

ولكون مسألة الملكيَّة الفكريَّة وتفصيلاتها، وحقوق التأليف وتشعُّباتها من المسائل المعاصرة التي لم تكن متداوَلة في تراثنا القديم بما هي عليه اليوم؛ فإنَّ الفقهاء المعاصرين عرضوا لهذه المسائل، في بحوث جادَّة، كثيرا ما عُرضت للنِّقاش والإثراء، مستندين في ذلك إلى أصل من أصول التَّشريع الإسلامي هو **الاستصلاح** أو **المصلحة المرسلة*** بحكم أنَّها الإطار الأنسب الذي تعالَج فيه مثل هذه المسائل، فعُقدت لذلك الملتقيات والمؤتمرات، واستُصدِرت فيها الفتاوى والتَّشريعات من ذلك: "**مؤتمر الحقوق المعنويَّة**" المنعقِد بالكويت في ثمانينيَّات القَرْن الماضي، والمؤتمر الدَّولي: "**اقتصاديَّات الدُّول الإسلاميَّة في ظل العولمة**" المنعقِد بالقاهرة من 17– 19 محرم 1420ه، الموافق: 3– 5 ماي 1999م ومؤتمر "**ندوة حقوق المُؤلف – مدخل إسلامي**" المنعقد بالقاهِرة في:1–2 يونيو 1996م من قِبل رابطة الجامعات الإسلاميَّة وإشراف جامعة الأزهر، والمؤتمر الدَّولي الرَّابع للفلسفة الإسلاميَّة "**الإسلام في عَصْر العولمة**" الذي عقدتْهُ كليَّة دار العلوم– جامعة القاهرة، في: 3–4 مايو 1999م. وكذا ما يصدر من مؤلَّفات، ومقالات تتناول جوانب مسألة أمن المعلومات، وحدود التَّعامل مع صورها ومستجداتها من الوجهة الشَّرعيَّة، وهي في مُجملها تقرُّ بحقوق المؤلِّفين على مؤلَّفاتهم، وتجريم الاعتداء عليها بغير الوجه الشَّرعيّ الذي لا يمكن أنْ يدَّعي أحدٌ ممَّن انتسب إلى العلم أنْ يجهله.

وفي بيان بعض وجوه هذه القضية يقول الأستاذ: عبد السَّلام داود العبادي ممثِّل الأردن في مجمع الفقه الإسلامي ونائب رئيسه: "الاستئثار المقصود في الملك في الفقه الإسلامي، ليس معناه احتواء الشَّيء من قبل المالك، إنَّما معناه أنْ يختصَّ به دون غيره؛ فلا يعترضه في التَّصرُّف فيه أحد. والتَّصرُّف يكون في الأشياء حسب طبيعتها، لذلك يختلف مدى التَّصرُّف في أنواع الملك في

الشَّريعة من نوع إلى أخر[11]" فينقل إقرار الشَّريعة الإسلاميَّة للنَّاس بأصل حقِّ التملُّك ورعاية تفصيلاته "فالتَّأليف مثلا كان عبارة عن شعور بالواجب ورغبة في الثَّواب والأجر، بل كان المُؤلِّف يحرص على نشره بكافة الطُّرق، لأنَّ في ذلك مزيدا من الأجر والثَّواب، وعليه لم تبرز فكرة استحقاق الشَّخص لما يُنتجه من أشياء غير مادِّية، وإنْ كانوا حريصين على نسبة الآراء إلى أصحابها[12]". وفي هذا التفاتة هامَّة في الإشارة إلى مسألة الاحتساب والرَّغبة في الثَّواب عند المؤلِّفين المسلمين التي يعتبرها الفقهاء المسلمون خصيصة للتّشريع الفقهيّ الإسلامي في مقابل التَّشريعات الوضعية التي تغلب عليها الوجهة المادِّية في تصنيف الحقوق وحمايتها، ومع ذلك فالتَّشريعات الإسلاميَّة تقف بلا تردُّد مع تجريم الاعتداء على حقوق المؤلِّفين، وترصُد لذلك العقوبات الرَّادعة شأنها في ذلك شأن كلِّ التَّشريعات التي تعرَّضت للظَّاهرة. وفي ذلك ينقل الأستاذ العبادي قول الدكتور محمد صادق فهمي: "ونعتقد أنَّ الرُّوح التي تهيمن على التَّشريع الإسلاميِّ؛ تأبى إلاَّ أنْ تعترف بحقوق المؤلِّفين، لأنَّ التَّشريع يأبى على الشَّخص أنْ يضرَّ بغيره، كما أنَّ **اغتيال مؤلف** إنْ هو إلاَّ سلوكٌ إجراميٌّ تأباه الشَّريعة الإسلاميَّة، وفي قول رسول الله: ﷺ **(لا ضرر ولا ضرار)** ما يكفي لحماية حقوق المؤلِّفين[13]" فمع أنَّ المسألة بتفصيلاتها من مستجدات الحياة المعاصرة؛ إلاَّ أنَّ استنطاق الفقهاء للنُّصوص الشَّرعيَّة في إطار القواعد الأصوليَّة والفقهيَّة الإسلامية، مكَّن من تحديد معالم الظَّاهرة، وإحاطتها بتوجيهات جاءت في البداية أخلاقية مهذبة، ثمَّ ثنت بالعقوبات الرَّادعة التي تُكيَّف إجراءاتها وأنواعها على مستوى الجهات القضائيَّة والعدليَّة، التي يسند إليه تأسيس هذه القضايا، وتعيين أطرافها، وترسيم معالم العلاقة القانونية بين المؤلِّفين والمتلقين.

2- أمن المعلومات من منظور القوانين الوضعيَّة والتَّشريعات الدَّوليَّة:

يحيل مصطلح أمن المعلومات على مصطلح أكثر شهرة وتداولا، وبه صيغت

الاتفاقيات، وسطِّرت التَّشريعات ذلك هو مصطلح "**الملكية الفكرية**" **الذي** تعرّف فيه مفرداتها بأنها: "الإبداعات التي ينتجها العقل من اختراعات ومصنَّفات أدبيَّة وفنِّية ومن رموز وأسماء وصور وتصاميم مستخدمة في التِّجارة، وتنقسم الملكيَّة الفكرية إلى فئتين هما:

الملكيَّة الصِّناعيَّة: وتضمُّ براءات الاختراعات، العلامات التِّجارية، والرُّسوم والنَّماذج الصِّناعيَّة والبيانات الجغرافيَّة.

حقٌ المؤلِّف: ويشمل المصنَّفات الأدبيَّة (كالروايات والقصائد الشَّعرية والمسرحيات) والأفلام والموسيقى، والمصنَّفات الفنِّيَّة (كاللَّوحات الزَّيتيَّة والصُّور الشَّمسيَّة والمنحوتات) والتصاميم العمرانية. وتشمل **الحقوق المجاورة** لحقِّ المؤلِّف، حقوق فنَّاني الأداء في أدائهم، ومنتجي التَّسجيلات الصَّوتيَّة في تسجيلاتهم وهيئات البث في برامجها الإذاعيَّة والتِّلفزيونيَّة[14]، وكانت طبيعة هذه الملكية وحداثتها النِّسبيَّة مقارنة بالقضايا الإنسانيَّة القديمة، مثار نزاع بين القانونيين، إذ مع إفرازات الحضارة الحديثة وتعقيداتها، واتِّساع شبكة العلاقات الإنسانيَّة زادت الحاجة إلى ضبطٍ أكثر للحقوق والالتزامات والتَّعرُّض للتَّفاصيل والحالات المستجدَّة، ولعلَّ تنازع القانونيِّين في إدراج وجهة الحقوق الفكرية ضمن الحقوق الشخصية أو الحقوق العينية، يرجع إلى طبيعة هذه الملكيَّة حيث إنَّ لها جانبا معنويا هامًّا إلى جانب قيمتها المادِّية، ولذلك أدرجت في قسم آخر وصنفت بموجبه تحت مسمًّى "الحقوق المعنوية" وهو تقسيم لم يسلم من الانتقاد بحكم استمرار الملكيَّة المادِّية للمنتج، بينما تنخلع عنه الملكيَّة المعنوية بعد فترة زمنيَّة تذهب تشريعاتٌ بأنّها خمسون سنة بعد وفاة المؤلف، ويقول التَّشريع الإسلامي بأنّها ستون عاما في أظهر أقوال المحدثين[15].

2-1- أمن المعلومات بين تخمة التَّشريعات وغياب المتابعات: شهد القران التاسع عشر (19) الميلادي اتِّفاقيات شهيرة تناول القائمون عليها طرائق حماية المؤلِّفين، وضمان أمن المعلومات وضمان براءات اختراعاتهم، إثر الانفجار

الصناعي والتكنولوجي الهائل الذي أعقب تمكُّن الثورة الصناعية في أوربا وبات سن تشريعات تؤمّن نسبةَ المعلومة إلى مصدرها بما يكفل حقَّ المصدر المادِّيِّ والمعنويِّ أكثر من ضرورة، بعد أن صارت هذا النتاج الفكري والعلمي مصدرا لثروات هائلة تنافست الشَّركات العالمية الكبرى في الظَّفر بعوائدها حتى إنَّ بعض القانونيين والحقوقيِّين يرون أنَّ هذه الاتفاقيات قامت في الأساس لحفظ حقوق الشَّركات الكبرى، وتأمين عوائد ممتلكاتها الفكرية والتجارية والصناعية المعنوية، أكثر من حفاظها على حقوق الأفراد.

وبعد أول وثيقة وطنية بريطانية سنة 1807م، أخذ الاهتمام بالظَّاهرة يتوالى، حتّى أصبح ذلك شأنا أوربيا في مدينة (برن) بسويسرا سنة 1886م وتجاوز الأمر بذلك شكل المحلِّية إلى الإقليميَّة تمهيدا للعالمية الّتي تقَارَب فيها الفكر الإنسانيُّ بفعل ثورة الاتِّصالات الرَّهيبة، والّتي يتداول فيها العالم النِّتاج العلميِّ العالمي في سهولة كبيرة، وسرعة لم تعهدها البشرية من قبل.

ولا تزال الاتِّفاقيَّات الدَّولية والإقليميَّة والتَّشريعات المحلِّيَّة والقطاعيَّة والمراسيم والمواد القانونيَّة تتوالى منذ ذلك العهد، ساعية إلى تنظيم العلاقة بين المؤلِّف المنتج للمعرف والمتلقي المستعمل لها موجِّهة أحيانا، ومتوعِّدة أحيانا ومنفِّذة للوعيد تارة أخرى، ومع ذلك فإنّ جرائم الإغارة على التَّصانيف والمؤلفات، وفضائح السرقات العلمية لا تزال تُزكِم روائحها النَّتنة الأنوف وعلى صروح أرقى مؤسسات المجتمع (الجامعات) وإنْ تفاوت حِدّتها من بلد إلى آخر بحكم ثقافة كلِّ بيئة، ومستوى وَعيها الفكريِّ والاجتماعيِّ، وكفاءة منظومتها الرقابية والقضائية، ومدى رغبة نخبها وأصحاب القرار فيها في التَّصدِّي للظَّاهرة والحدِّ من آثارها، فإذا بلغت بعضُ البيئات الغربيَّة حدّا مقبولا في استقباح هذا الفعل والأخذ على أيدي أصحابه في جرأة وصرامة؛ فإنّ كثيرا من المجتمعات المتخلِّفة والنَّامية ومنها الدُّول العربية الإسلامية لا يزال التَّعامل

فيها مع هذه الجريمة محدودا، وقد يبلغ في بعض الحالات حدَّ التَّواطؤ المقرف والصَّمت الدَّنيء.

يستعرض ابن خلدون ما كان سائدا في الزَّمن الإسلامي الّذي انتشرت فيه العلوم واتَّسعت دائرة التَّأليف، وراجت سوق تناقل المعارف وأدائها فيقول: "ثم وقفت عناية أهل العلوم وهمم أهل الدول على ضبط الدَّواوين العلميَّة **وتصحيحها بالرِّواية المسندة إلى مؤلفيها وواضعيها**، لأنَّه الشَّأن الأهمُّ من التَّصحيح والضَّبط، **فبذلك تُسند الأقوال إلى قائلها**[16]". والنَّص صريح في وصف الحالة الّتي عليها تناقُل العلوم، إذ عرف ذلك الزمن بالضَّبط والدِّقَّة، وإذا كان هذا وصفا لحال تناقُل العلوم فإنّ وصف الدَّولة العام، هو بلوغ الجماعة الإسلاميَّة أوج سُؤددها في العراق والأندلس، ومن خلفهما بقية حواضر العالم الإسلامي وأقاليمه "ولهذا نجد الدَّواوين المنسوخة لذلك العهد في أقطارهم على غاية من الإتقان والإحكام والصِّحَّة[17]" ولكن هذا الوضع لم يدم طويلا، فمع تردِّي الوضع العام للدَّولة، تردَّت معه كلُّ مظاهر الحياة الأخرى ومنها الحياة العلميَّة "ولقد ذهبت هذه الرُّسوم لهذا العهد جملة بالمغرب وأهله لانقطاع صناعة الخطِّ والضبط والرِّواية منه بانتقاص عمرانه وبداوة أهله[18]" وهو بذلك يقرِّر حقيقةً اجتماعيَّةً تقضي بأنّ قوة المظاهر العلميَّة والفكريَّة في المجتمعات وارتقاءها، أثرٌ مباشرٌ لقوَّة حضارة تلك المجتمعات وارتفاع تفكير نُخبِها، فلا مكان فيها للأدعياء والسُّفهاء والمتسلِّقين، وهي الصُّورة الّتي تتكرَّر في العصر الحديث، إذ تلتصق ظواهر الانتحال والسَّلخ والسَّلب العلمي والفكريِّ أكثر بالدُّول المتخلِّفة والمجتمعات التَّابعة والّتي تقف في صفوفها الأولى المجموعة العربية الإسلامية.

ومع هذا الجو العام فإنَّ محاولات محتشمة، ومبادرات تحتاج إلى إنجاز الجزء الأخير منها دائما تقف التشريعات العربية في مجال حماية المعلومات عاجزة عن تفعيل ما أنجز من تشريعات، ومتابعة الكم الهائل من الخروق

المتسارعة للتشريعات السماوية والأرضية في هذا المجال، وبتصفح سريع للأمر رقم 97-10 مؤرخ في 27 شوال عام1417 الموافق 6 مارس سنة 1997م المتعلق بحقوق المؤلف والحقوق المجاورة الجزائري، على سبيل المثال لا الحصر، ومع الملاحظة الأولى بشأن صدوره المتأخِّر جدا (1997م) فإنّه مشروع يتفق مرّة أخرى مع الشرائع السماوية واللوائح والاتِّفاقيَّات الدَّولية في تنظيم العلاقة الحسَّاسة والدَّقيقة بين الحقِّ الطَّبيعيِّ للمؤلِّف في حماية ملكيته على نتاجه ويثبت الإقرار بواجب المؤلف والمبدع نحو الجماعة الإنسانية وإمدادها بما تقتضيه مظاهر التَّعايش الجمعيِّ لبني الإنسان، في الوقت الّذي تطالَبُ فيه الجماعة الإنسانيَّة الباحثة عن المعارف والعلوم في مؤلَّفات نُخبها بالإقرار بفضل تلك النُّخب، وحقِّ عناصرها في آثارها وعوائدها، والّذي يأخذ صورا فصَّلت التَّشريعات أصلها العام: "ذكر اسم المؤلف والمصدر" لتعمل بعد ذلك تفاصيل منهجيَّةُ إعدادِ البحوث والرَّسائل والكتب عَمَلَها في بيان كمِّية المنقول، ونوعيَّة توظيفه، وصور الإحالة عليه، وغير ذلك من تفاصيل لم تَدَعْ مساحة لأيِّ عدوانٍ يَطَال الباحثين وأعمالَهم، أو تُحرَم بمقتضاه الجماعة الإنسانية من شيوع المعارف ومنطقيَّة توظيفها واستثمارها، من ذلك مثلا ما تضمَّنه الفصل الثَّالث الوارد بعنوان: الاستثناءات والحدود، في مواده من (33 إلى 54) من الصِّيغ الّتي يمكن الاستفادة من خلالها من المؤلَّفات والتَّصانيف دون المساس بالحقوق المادِّية والمعنويَّة للمؤلِّف الأصليِّ كإجراءات تراخيص التَّرجمة، وحدود استخدامها، وكيفيَّات استفادة المتلقِّين الخواص أو العموميِّين من العمل الفنِّي أو الأدبي، والمواد في عمومها محاولة تبدو عليها الرغبة في حفظ الحقوق الطَّبيعيَّة الفرديَّة للمبدعين والمؤلِّفين، ورسم معالم منتَظَمة تمكِّن المتلقِّين من حقِّهم في الاستفادة المعقولة من محتويات الأعمال وهي إلى ذلك أيضا مواد تشريعيَّة اجتهدا واضعوها في التَّركيز على أمرين متقابلين بحيث لا يبغي أحدهما على الآخر.

أ- حقُّ المؤلِّف على الجماعة في حماية جهده الفكريِّ بشقَّيه المادِّي والمعنويِّ بتفصيلاتهما.

ب- حقُّ الجماعة في الاستفادة المعقولة من محتويات المصنَّفات استفادة مقيَّدة بأخلاقيَّات وأعراف معلنة.

وتضمن الفصل الرَّابع من الأمر نفسه، مدَّة الحماية الَّتي تكفلها القوانين لصاحب الحق ولورثته وسواء كان تصنيفا فرديا أو جماعيا تناولت المواد (55-56-57) ما يُرى أنّه محاولة لحصر صور التَّعامل المحتملة مع المؤلَّفات وتقنينها بل تجاوزت ذلك إلى حماية المصنَّفات المنشورة بأسماء مستعارة أو مجهولة المؤلِّف في المادة (58) وبصرف النَّظر عن تفصيلات نصوص هذه المواد فإنّها تتَّجه في روحها إلى دعم قيم احترام ملكيات الآخرين حتّى ولو كانوا غير معروفين بالتَّعيين، وغرس مبدأ أدب احترام الباحثِ نفسَه، وهو التزام أخلاقي راق قبل أنْ يكون إلزاما قانونيًّا مُجبرا، وكلُّ ذلك خلال مدَّة زمنيَّة تسمح لصاحب أو أصحاب الحقِّ التَّمتُّع بالجزء الشَّخصيِّ من ثمرات المصنَّف المادِّية والمعنويَّة، ولكن أين يمكن رؤية أثر هذه النُّصوص وغيرها في ميدان يستغيث فيه المتعرضون لسرقة رسائلهم وأطروحاتهم ومقالاتهم، ولا مجيب، وتزداد فضائح السرقات (غير العلمية) ازديادا مطَّردا أصبح يخشى من أنْ يصبح الأصل وما دونه استثناء.

3- أمن المعلومات من منظور السرقات الأدبية وقضايا الأدب المقارن:

يحلو للكثير ممَّن يستصغرون جرم تهديد الأمن المعلوماتيِّ التَّذرُّع بوجود ظاهرة السَّرقات عبر تاريخ الإنسان العلميِّ والفكريِّ والفنِّيِّ، ويُغرِقون في الاستشهاد على أنّ الأمر موجود بالقُوَّة والفعل وبذلك فما على المجتمع العلميِّ أن يقبل به، أو أن يقبل التعايش معه، فهل استدلال هؤلاء بذلك له مبرِّر يقوم عليه؟ وهل الاستشهاد بقضية السرقات الأدبية، وقضية التأثر والتأثير بين الآداب المقارنة سند صحيح لقياس السرقات العلمية المعاصرة عليها؟.

3-1- بين السَّرقات الأدبيَّة في التُّراث، والسَّرقات العلميَّة في الوسط العلميّ المعاصر: لا شك أنّ مسألة السَّرقات الأدبيَّة قد شغلت نفرا كثيرا من الأدباء والشُّعراء والنُّقاد، وملأت حيِّزا معتبرا من مكتبتنا العربية القديمة والحديثة؛ ولكن الّذي يجب اعتباره عند المقارنة هو الوقوف على مستويات الشَّبه والاختلاف بين الظَّاهرتين، ويبدو أنّ هناك اختلافا كبيرا لا مجال فيه للمقارنة من وجوه.

أ- لا تكاد ظاهرة السَّرقات القديمة تُدرج إلاَّ في سياق قضايا نقديَّة شهيرة أخرى، كقضايا **القديم والحديث**، و**اللَّفظ والمعنى والطبع والصَّنعة**، وغيرها من القضايا الّتي تشكلت فيه النَّظرة إلى السَّرقات نتيجةً لإبداعٍ أدبيٍّ وشعريٍّ متفجِّرٍ، وحراكٍ ثقافيٍّ هائلٍ شهدت فصوله فترات العهد العباسي، فيذهب إحسان عباس إلى أنّ مُحصِّلة استفحال هذه الظَّاهرة كقضية نقديَّة هي "أنَّ الشَّاعر المُحدَث قد وقع في أزمة تحدُّ من قدرته على الابتكار، ولهذا فهو إمّا أنْ يأخُذ معاني من سبقه، أو يولِّد معنى جديدا من معنى سابق[19]" وعلى هذا الأساس لم تكن السَّرقات الشِّعريَّة مجرَّد إغارة على نتاجٍ سابقٍ، بقدر ما كانت تحوُّلا خطيرا في طرُق الصِّياغة والبناء اللَّفظيِّ والمعنوي، وقد غذَّى ذلك صراعٌ فكريٌّ ومجتمعيٌّ كبيرٌ، وكان -أيضا- استجابة لجدلٍ نقديٍّ حادٍّ بين تشكيلات علميَّة مختلفة المشارب والتوجّهات فكان أعلامها قامات الإبداع الأدبيِّ والفنّي العربيِّ القديم، ولذلك تلطَّف الكثير من الدَّارسين في إطلاق مصطلح "السَّرقة" مستعيضا له بـــ "التَّضمين" أو "حسن الأخذ" أو غيرهما[20]، وكأنّهم بذلك يطلبون شيئا من العذر لكثير من الحالات الّتي تعفُّ أن تنزل إلى منزلة السَّرقة.

أمّا تهديد الأمن المعلوماتي العام، والتعرُّض لنتاج المبدعين والمؤلفين والباحثين في العصر الحديث بالصورة التي شاعت، فتختلف مظاهره ودوافعه وأحجامه بحيث لا يمكن مقارنته بما سبق به الحديث عن السَّرقات الأدبيَّة فمظاهر هذه السَّرقات اقتطاع بالجملة لمباحث أو فصول، وربَّما مذكِّرات

بأكملها وتبنِّيها دون تردُّد أو خجل، فقبُحَت هذا الأفعال مظهرا ومقدارا، والأقبح من ذلك تلك التَّبريرات الّتي يحاول المُغِيرون إقناع أنفسهم بها، كاستكمال الأعمال الّتي حُدِّدت لها آفاق زمنيَّة معلومة، أو ترتيب مقابل ماديٍّ أو وظيفيٍّ وشتان بين سرقة وسرقة.

ب- إنّ سرقات الأوَّلين وإنْ كانت تحت هذا المسمَّى؛ فإنّها لا تُشبِهِ السَّطو الّذي ابتُلِي به البحث العلميُّ والأكاديميُّ المعاصر، إذ يشيع في تقسيم النُّقَّاد للسَّرقات الأدبيَّة أنواع وأقسام، مستحسنة عند بعضهم ومذمومة عند آخرين ولكنّها مع ذلك تشعُّ بالحركة والإبداع حين يتابع النُّقَّاد نتاج هؤلاء فيصنِّفونه إمّا إيجازا لمُطوَّل، أو تحسينٍ لمرذولٍ، أو استخراج لخفيٍّ، أو بالزيادة أو النقصان أو غير ذلك من الحركيَّة الّتي لم يُبقِ اللاحق فيها ما سُبِق إليه؛ بل زاد وولّد وليست هذه الورقة في معرض التَّخطئة لهذا أو التَّصويب لذاك ممَّن عدَّ ذلك سرقة أم لا، فذلك خلافٌ مبسوطٌ في مظانِّه، ولكن الظاهر أنَّ لا وجه للشبه بين ما عرف بالسرقات في التراث، وبين الجرائم النَّتنة للسَّطو الّذي يطال جهود الباحثين من قبل زملائهم، كما أنَّه لا سند للقياس بين جرائمهم وبين السرقات الّتي يتذرَّعون بها فهذا سطو لا إبداع فيه ولا خلق، بل هو انتهازية وتسلُّق لا تبرِّره الرَّغبة في العلم، ولا يشفع له إثراءٌ للمعرفة، ذلك أنّ أكثر ما يُنشر من مواضيع السَّطو هو المقالات المحكّمة، أو الرَّسائل الجامعيَّة والدَّافع من ورائها هو نيل شهادة، أو تحصيل رتبة أو وظيفة، وشتان بين أخذٍ شريف الغرض دافعه استثارة القرائح، وتوليد المعاني وتوسيعها، والاستمتاع بتقليب وجوهها وبين جرم يُغِير فيه عاجز وصوليٌّ متسلِّق، يَغرِف جُهودَ من سبقوه لغرضٍ أسفل من سببه.

ج- إنّ سرقات الأوَّلين عُدّت بإجماع النُّقاد قضية نقدية أثرى منها الشِّعر والأدب والنَّقد، وأثارت حفائظ الإبداع والابتكار، كما أغرت النُّقَّاد بمتابعة الظَّاهرة بما أثرى الدَّرسَ النَّقديِّ والبلاغيَّ برمَّته فأفاض العلماء في وضع

المقاييس النَّقديَّة، وفصّلوا معايير القضية وأساليبها، واستغْنَت السَّاحة النَّقديَّة بعشرات المصطلحات النَّقدية، وبمثلها من آراء ابن جني وأبي هلال العسكري وابن قدامة والآمدي والجرجانيَان عبد العزيز وعبد القاهر وابن سنان والسكاكي والعميدي وابن رشيق وغيرهم، فغشيت مؤلَّفاتهم مصطلحاتٌ كـ: الإحالة والتغيير، والمولد، والحذف، والزيادة، والحمل على المعنى والاصطراف والانتحال، والإغارة، والغصب، والمرافدة، والاهتدام، والإلمام، والاختلاس والعكس والموارَدة، والالتقاط، والتَّلفيق، والمجدود... وغيرها الكثير* وحظيت هذه المصطلحات بالشَّرح والتَّمثيل من شعر العرب واستخراج وجه كلِّ مصطلحٍ وأثره. فما الّذي أضافته اختلاسات فصول من مذكرات وورقات كاملة بلا إحالة إلى مصدرها، بل تعدَّى الأمر إلى سلخ مؤلفات من الغلاف إلى الغلاف؟ أليس ذلك سوى قعودا عن البحث، وتكرارا ممجوجا للمعارف وركونا إلى كلِّ مستهلَكٍ سابقٍ؟ فكان من نتائج ذلك ترهُّل البحث العلميِّ برمته وتلبّس القلَّة المُجدَّة باليأس من آفاق مشرقةٍ لبحوثهم وإنجازاتهم مقابل تنمُّر مقتنصي درر غيرهم، والسَّالبين لحقوقهم، والمختطفين لثمرات الأذهان وعصارات العقول، فأصاب ساحة البحث العلمي الدَّخلُ والدَّخَن، ولم تَصِرْ خالصة لأهلها.

3-2- أمن المعلومات ومسألة التأثُّر والتَّأثير بين الآداب: مثَّلت قضية التَّأثر والتَّأثير في آداب الإنسانية وآثارها شكلا من أشكال التَّقارض المعرفي بين الحضارات والشُّعوب، وتعِزُّ عن الحصر الآثارُ الّتي تتبَّع فيها النُّقاد والدَّارسون ملامح -قد تقل وقد تكثر- لأعمال أخرى سابقة، باللّغة نفسها أو بلغات مختلفة، فآثار نُصوص وأعمال أدب الرَّافدَيْن القديم ومصر وسوريا على الآداب البهلوية والعبرية واليونانية والرومانية، وأثر الأدب اليونانيِّ والرُّومانيِّ على الأدب الأوربِّي الحديث، وأثر الأدب العربي ولغته على الأدب العبري والفارسي والهندي والأوربي، وأثر أدب النَّهضة الحديثة في أوربا على الأدب

العربي، وغير ذلك من آثار الآداب في آسيا وأمريكا، كلّها شواهد على استحالة محاصرة المعرفة، ولا يمكن ضبط مساراتها وقَصْرها على أصحابها وأزمنتها وأماكنها، فصارت لذلك بحوث الأدب المقارن بوصفه علما "يبحث عن التَّأثُّر والتَّأثير في الأدب على جميع المستويات، سواء أكان ذلك بين كاتب وكاتب، أم بين تيَّار فكريٍّ وتيَّار فكريٍّ آخر، كما أنّه يبحث في انتقال الأنواع الأدبيَّة من أمَّة إلى أمَّة، وفي الأخذ والعطاء بين الشُّعوب على مختلف مراحل نموِّها[21]" مجالا خصبا لمتابعة مظاهر التَّأثُّر والتَّأثير بين الآداب الإنسانيَّة على أنّها شكل من أشكال الاقتباس والنَّقل، وإن بدا أقرب إلى الإبداع منه إلى السَّرقة أو السَّطو، وبات إقرار النُّقاد وعلماء الأدب المقارن بوجود هذا الأمر حقيقة قائمة، فراحوا يُوجِّهون لها الأسباب والمظاهر، ويصنِّفون أنواع الاقتباس، يقول محمد غنيمي هلال: "وأول ما يلفت نظر الباحث ويدفعه إلى استطلاع معالم الصِّلات الأدبيَّة، هو التَّشابه في النُّصوص لكاتبَيْن أو لعدَّة من الكتَّاب في آداب مختلفة تشابُها يحمل على الظَّنِّ بأنّ هناك صِلاتٍ تاريخيَّة بين هؤلاء الكتَّاب[22]" والنَّص صريح في القبول الواضح لهذا النَّوع من التَّأليف على أنّه شكل من أشكال تأثُّر الثَّقافات ببعضها البعض، وأخذ بعضها من بعض، من دون أنْ يجد دارسوا هذا النَّوع من الأدب غضاضة في ذلك، وغير ناظرين له بعين الرِّيبة في اعتباره سرقة أو عدوانا، بل عُدَّ شكلا من أشكال خدمة الآداب لبعضها، وسعي أهلها للارتقاء بها، ويستعرض الدَّارسون لهذا الجانب تواريخَ تأليف الأعمال لإثبات سابقها ولاحقها، وملاحظة القرائن لإثبات نوع الصِّلات وحجمها، وهل هو تأثُّر فعليٌّ، أم استجابةٌ لملابساتٍ متشابهة ولّدت أفكارا وأنساقا تعبيريَّة متماثلة؟ أم أنّه مجرد اتِّفاقٌ اصطلح عليه عند هؤلاء بـــ "توارد الأفكار" الّذي يتخذونه وجها من وجوه تبرير تشابُه النُّصوص والآثار.

ومن خلال كلِّ ما سبق نقف على أنّ دارسي هذا النَّوع من العلاقات بين الآداب والآثار، والقائمة أساسا على الاقتباس ونقل اللاَّحق عن السَّابق، لا

يعتبرون ذلك سرقة ولا عدوانا، بل يؤسِّسون له على أنّه علم له مبادئُه ومواضيعه وهدفه ومنهجه، وهي عناصر تتابع "انتقال" النُّصوص و"الأخذ والعطاء" بين الثَّقافات، وباستعراض حجم هذه المبادلات، نقف على كمٍّ هائلٍ من النِّتاج الثَّقافي للشُّعوب قد قام بالأساس على "النَّقل" عن الآخر*

غير أنّ الأعمال اللاحقة المتأثِّرة سلمت من الرَّمي بالسَّرقة والاختلاس بفعل احتفاظها بشخصيتها حاملة للسان أمّتها وثقافتها، متشبِّعة بروح كافية من الإبداع اللّغوي والفنِّي، وكأنّها لم تأخذ من السَّابق إلاّ ما هو حق إنسانيٌّ مشاع، وملكيَّة جماعيَّة لبني البشر، ولكلِّ أمة أو ثقافة أنْ تصبغه بصبغتها وتجتهد في صياغته بما يلائمها، وتلك معالم كافية للخروج بالأعمال المتأثرة من الدوائر المعيبة للسرقات.

ولك أنْ تنظر – مثلا– في رسالة الغفران لأبي العلاء المعري (449هـ–1057م) وهي أثرٌ أدبي عربي إسلامي صريح، نال فضل السَّبق التَّاريخيِّ والفنِّي، وصِيغَ في حدود الثَّقافة الإسلاميَّة وشخوصها وأعرافها وعقائدها في القرن الخامس الهجري/الحادي عشر ميلادي، وتنظر للكوميديا الإلهية الشهيرة لـ (Dante Alighieri) دانتي أليغييري (721هـ/1321م) المصنَّفة في القرن الثَّامن الهجري/الرابع عشر الميلادي، وبينهما نحو (3) ثلاثة قرون، وقد عدّت الأولى سلفا تاريخيًّا وثقافيًّا ومعرفيًّا للثانية، رغم ما يصر عليه المستكبرون من نفيٍ لهذا التَّأثُّر بدافع عصبيٍّ لا علاقة له بالعلميَّة، ومع ذلك فإنّ أحدا من الدَّارسين لم يرمِ دانتي بالسَّرقة، بل عُدَّ ذلك "تأثرا" طبيعيًّا بين الثَّقافات والشُّعوب، ومنزلة الكوميديا بين الآثار أشهر من أن يذكر، لكونها عملا آخر اكتسب شخصيته وروحه وإبداعه من جهد صاحبه، فأين السَّرقات العلميَّة الّتي يئن البحث العلميُّ والأدبيُّ تحت وطأتها في جامعات البلاد المتخلِّفة، ومنها البلاد العربيَّة والإسلاميَّة؟ وأين التَّحويل الحرفيُّ للأطروحات والمقالات دون

إقرار بالأصل، أو إحالة على المصدر، من تلك النماذج الرّاقية فنيًّا وأدبيًّا في الآداب العالمية المقارنة؟

الخاتمة: تحتل مسألة أمن المعلومات مساحة ذات شأن في الوجهة العلمية للأمم، فعلى قدر كفاءة المنظومة التعليمية والفكرية، وعلى قدر صرامة الجهات التشريعية والرقابية والقضائية للدُّول؛ تشيع التقاليد العلمية التي تمهِّد للانطلاق الحضاري، وتسهم في استدامة الشهود الحضاري، كما أنَّ ترهُّل طرائق البحث العلمي، وضحالة مستوياته، وتردُّد نخبه، وتفشي الرَّداءة العلمية، وقصر الرؤية المجتمعية للدول في ما يتعلق بترقية حقيقية وجادَّة للبحث العلمي وأدواته ومؤسساته، يعدُّ معيارا حقيقيا لتخلُّف المجتمع، ومسبارا صادقا للمسافة بينه وبين الحضارة.

إنَّ من الوسائل ذات الأثر في تعزيز أمن المعلومات في المجتمعات العربية والإسلامية هو عدم التَّردُّد في استخدام آليات وإجراءات التَّربية الخلقيَّة المستمدَّة من الأصول العقدية للإسلام، وليس أفضل للباحث من يكون عليه من نفسه رقيب، ولا أضمن للبحث العلمي الأمين من أن تكون وجهته الأولى هي الاحتساب والثواب قبل أن يكون وجهته العوائد المادية والثمرات العاجلة، فلقد كان شرف الأداء ونزاهة التحمُّل السبب الرئيس في تأمين المعارف والعلوم على العهد الإسلامي الأول، مرتكزا في طرفه الأول على حرص المعلِّمين والمصنفين على أداء علومهم لتحقيق النفع العام انطلاقا من أنَّهم حملة ميراث وبُناة حضارة، وفي طرفه الثاني على أمانة المتلقِّين ونزاهة تحمُّلهم، حين تعلَّموا خلق التَّعلُّم قبل طلبه، وأيقنوا حقيقة دورهم في أنَّهم مسؤولون عما تحمَّلوا، فقصروا هممهم على ذلك.

ولعل من المعايير العامة التي يحسن بالباحثين إشاعتها بعد الأخذ بها في مجال الاتكاء المعرفي على الآخرين، أنْ ينظر في طبيعة الأخذ، فإنْ كان سندا لمعرفة جديدة، أو قاعدة لبناء فكري آخر، أو رائزا لإضافة ما؛ فذلك محمود

يصنَّف ضمن ترقية العلوم واستثمارها وإشاعتها، على أنْ يعتمد المنهج الشَّكلي المعروف الذي يحدِّد كمَّ المأخوذ ونوعه وطريقته مُسندا إلى القواعد المنهجية الشَّكليَّة العالمية.

إنّ ممّا يجب أن تقوم عليه المنظومات التَّربوية السليمة في ما يتعلق بأخلاقيات البحث العلمي هو تعويد التلميذ مبادئ التعلّم وقواعد الاستفادة من الآخرين منذ المراحل التَّعليميَّة الأولى، والتَّعامل في ذلك بصرامة توازي صرامة التَّلقِّي نفسه، حتّى إذا تقدم المتعلِّم في أطوار التَّعليم تخلَّق بأخلاق الأخذ عن الآخرين، وتملَّكه شعور الحرج من أنْ ينسِب إلى نفسه ما ليس له، بفعل استقباح البيئة التَّعليميَّة لذلك، والتَّشنيع على فاعليه، ومقابل ذلك تعمل هذه البيئات على تكوين المتعلّم تكوينا يمتلك فيه القدرة على استغلال مساحات ما بين الاستشهادات والاقتباسات بجودة التَّعليق، وصرامة التَّحقيق، ودقَّة التَّحليل ووجاهة التَّعليل، وجودة الاستعراض، وسلامة المقابلة، وحصافة التَّعقيب وذكاء الرَّدِّ بالموافقة والتَّأييد أو الاعتراض والتَّفنِيد، يصحب ذلك أدبٌ جم في مناقشة الأقوال، وخلق كريم في إبداء الآراء وتواضع في إصدار الأحكام وترفُّق في تقليب الوجوه، فيكتسب المتعلّم مع العلوم والمعارف أخلاقها وأدب التعامل مع أصحابها ولكَمْ أوصى الحكماء مريديهم بالعلم والخلق معا إذ بهما – معا– التَّمام.

إنّ أعظم مصاب نزل بما بقي من العلم في مؤسساتنا التَّعليميَّة هو تحويله إلى مطيَّة بلا خلق، ووسيلة بلا شرف، وأداة بلا كرامة، فسُلِب قيمته الّتي يُكرَّم فيها المتعلِّم بشرف طلبه، ويُكرَّم فيها المعلّم بصدق عطائه، وتمالأ القوم –كلٌّ من موضعه– على سلب العلم كريم قيمته، وشريف فضله فهانت دون ذلك وسائل طلبه، ولانت طرائق تحصيله، ولا عجب بعد ذلك أن ترى وتسمع عجائب السَّلخ وغرائب الإغارة ومضحكاتٍ مبكياتٍ من غباء الاستنساخ وحمق الاستلحاق، فضاعت بذلك هيبة بعض النُّخب، بعد أنْ ضاعت أخلاقهم، وصار

معقد الأمل في صلاح الأمّة وإصلاحها مصدرا لدائها وبلائها، ومن ذا يصلح الملحَ إذا الملحُ فسد.

قائمة المصادر والمراجع:

- القرآن الكريم.

1. إحسان عباس، تاريخ النقد الأدبي عند العرب، ط2.عمان: 1993م، دار الشروق.
2. إسماعيل أبو الفداء بن كثير، تفسير القرآن العظيم، تح: سامي بن محمد سلامة، ط2. الرياض: 1420هـ- 1999م، دار طيبة للنشر والتوزيع.
3. بدوي طبانة، السَّرقات الأدبية دراسة في ابتكار الأعمال الأدبية وتقليدها دط. القاهرة: دت، نهضة مصر للطباعة والنشر والتوزيع.
4. جمال الدين أبو الفرج بن الجوزي، زاد المسير في علم التفسير، تح: عبد الرزاق المهدي، ط1. بيروت: 1422 هـ، دار الكتاب العربي.
5. الحسن أبو علي بن رشيق، العمدة في محاسن الشعر وآدابه ونقده، تقديم وشرح وفهرسة: صلاح الدين الهواري/هدى عودة، دط. بيروت: 2002م دار ومكتبة الهلال للطباعة والنشر.
6. الحسين أبو محمد البغوي، معالم التنزيل في تفسير القرآن، تح: عبد الرزاق المهدي، ط1. بيروت: 1420 هـ، دار إحياء التراث العربي.
7. داود سلوم، الأدب المقارن في الدراسات المقارنة التطبيقية، د ط. القاهرة: 1424هـ/2003م، مؤسسة المختار للنشر والتوزيع.
8. عبد الرحمان بن خلدون، المقدمة، ط1. دمشق: 1426هـ/2005م مؤسسة الرسالة ناشرون.
9. عبد الرحمن أبو زيد الثعالبي الجواهر الحسان في تفسير القرآن، تح: محمد علي معوض /عادل أحمد عبد الموجود، ط1. بيروت:1418 هـ دار إحياء التراث العربي.

10. عبد الوهاب خلاف، علم أصول الفقه، ط1. الجزائر: 1990م، مكتبة الزهراء للنَّشر والتَّوزيع.
11. علي بن خلف ابن بطال أبو الحسن، شرح صحيح البخارى، تح: أبو تميم ياسر بن إبراهيم، ط1. الرياض: 1423هــ– 2003م، مكتبة الرشد.
12. فخر الدِّين أبو عبد الله الرازي، مفاتيح الغيب، ط3. بيروت: 1420ه، دار إحياء التراث العربي.
13. مجلة مجمع الفقه الإسلامي، جدة: منظمة المؤتمر الإسلامي: مج5 ص2014.
14. محمد الطاهر بن عاشور، التحرير والتنوير، دط. تونس:1984 ه، الدار التونسية للنشر.
15. محمد غنيمي هلال، الأدب المقارن، ط5. بيروت: د ت، دار العودة ودار الثقافة.
16. ويبو، ماهي الملكية الفكرية؟ منشور رقم (ISBN 978-92-805-1158-1 450A

المواقع الإلكترونية:

17- www.alukah.net/sharia

18- www.mediafire.com.

19-www.wipo.int.

20-www.e-lawyerassistance.com

الهوامش:

1 - جمال الدِّين أبو الفرج بن الجوزي، زاد المسير في علم التَّفسير، تح: عبد الرَّزاق المهدي، ط1. بيروت: 1422ه دار الكتاب العربي، ج1، ص 358.

2 - أبو زيد عبد الرحمن الثَّعالبي، الجواهر الحسان في تفسير القرآن، تح: محمد علي معوض /عادل أحمد عبد الموجود ط1. بيروت: 1418هـ، دار إحياء التراث العربي، ج2 ص147.

3 - أبو عبد الله فخر الدِّين الرَّازي، مفاتيح الغيب، ط3. بيروت: 1420هـ، دار إحياء التراث العربي، ج9، ص456.

4 - محمد الطاهر بن عاشور، التَّحرير والتنوير، د ط. تونس: 1984 هـ، الدَّار التُّونسية للنَّشر، ج4، ص192.

5 - المرجع نفسه، ص193.

6 - أبو محمد الحسين البغوي، معالم التَّنزيل في تفسير القرآن، تح: عبد الرَّزَّاق المهدي ط1. بيروت: 1420 هـ، دار إحياء التراث العربي، ج1، ص554.

7 - صهيب عبد الجبَّار، الجامع الصحيح للسُّنن والمسانيد، www.mediafire.com، ج9 ص322.

8 - رواه مسلم برقم (2129) من حديث عائشة.

9 - أبو الفداء إسماعيل بن كثير، تفسير القرآن العظيم، تح: سامي بن محمد سلامة، ط2. الرياض: 1420هـ- 1999م دار طيبة للنشر والتوزيع، ج2، ص181.

10 - ابن بطال أبو الحسن علي بن خلف، شرح صحيح البخارى، تح: أبو تميم ياسر بن إبراهيم، ط1. الرياض: 1423هـ- 2003م، مكتبة الرشد، ج7، ص347.

* المصلحة المرسلة هي: المصلحة التي لم يشرع الشارع حكما لتحقيقها، ولم يدل دليل شرعي على اعتبارها أو إلغائها. وسميت مطلقة لأنها لم تقيد بدليل اعتبار أو دليل إلغاء. ومثالها المصلحة التي شرّع لأجلها الصحابة اتخاذ السجون أو ضرب النقود، أو إبقاء الأرض الزراعية التي فتحوها في أيدي أهليها ووضع الخراج عليها، أو غير هذا من المصالح التي اقتضتها الضرورات، أو الحاجات أو التحسينات ولم تشرع أحكام لها، ولم يشهد شاهد شرعي باعتبارها أو إلغائها. (عبد الوهاب خلاف، علم أصول الفقه، ط1. الجزائر: 1990م، مكتبة الزهراء للنَّشر والتَّوزيع، ص81).

11 – عبد السلام داود العبادي "الفقه الإسلامي والحقوق المعنوية" مجلة مجمع الفقه الإسلامي، جدة: منظمة المؤتمر الإسلامي: مج5، ص2014.

12 – المرجع نفسه، ص2014.

13 – عبد السَّلام داود العبادي "الفقه الإسلامي والحقوق المعنوية"، ص2014.

14 – منشور الويبو رقم: ISBN 978-92-805-1158-1 450A) www.wipo.int، ص2.

15– أحمد يوسف سليمان "حقُّ المؤلِّف بين فقه الإسلام وفكر العولمة" www.alukah.net/sharia بتاريخ: 2015/09/12. 23.34سا.

16 – عبد الرَّحمان بن خلدون، المقدِّمة، ط1. دمشق: 1426هــ/2005م، مؤسَّسة الرِّسالة ناشرون، ص440.

17 – ابن خلدون، المقدِّمة، ص440.

18 – المصدر نفسه، ص440.

19 – إحسان عباس، تاريخ النقد الأدبي عند العرب، ط2. عمان: 1993م، دار الشروق، ص 671.

20 – بدوي طبانة، السَّرقات الأدبيَّة دراسة في ابتكار الأعمال الأدبيَّة وتقليدها، د ط. القاهرة: د ت، نهضة مصر للطِّباعة والنَّشر والتَّوزيع، ص161.

* – ينظر في تفصيل ذلك: أبو علي الحسن بن رشيق، العمدة في محاسن الشِّعر وآدابه ونقده، تقديم وشرح وفهرسة: صلاح الدِّين الهواري/هدى عودة، د ط. بيروت: 2002م، دار ومكتبة الهلال للطِّباعة والنَّشر، ج2، ص421 وما بعدها.

21 – داود سلوم، الأدب المقارن في الدِّراسات المقارنة التَّطبيقيَّة، د ط. القاهرة: 1424هــ/2003م، مؤسسة المختار للنَّشر والتَّوزيع، ص11.

22 – محمد غنيمي هلال، الأدب المقارن، ط5. بيروت: د ت، دار العودة ودار الثَّقافة ص330.

* – للوقوف على نماذج كثيرة ومختلفة من نوع النقل وحجمه في آثار الشعوب وثقافاتها ينظر كتاب: الأدب المقارن في الدِّراسات المقارنة التَّطبيقية لـــ: داود سلوم.

الأخطار والمشاكل المعاصرة الّتي تواجهها الأنظمة المعلوماتيّة (الفيروسات Les Virus وقرصنة المعلومات)

أ. وردية قلاز

ج/مولود معمري، تيزي–وزو

مقدّمة: تحوي شابكة الإنترنيت العالميّة على بنك من المعلومات الضّخمة يستطيع المتصفّح من خلالها تحميل أنواع من المعطيات تتراوح بين الموسوعات إلى قواعد المعطيات، مرورا بمختلف البيانات بسرعة مذهلة وآنية، فإذا كانت هذه الشابكة قد أحدثت ثورة معلوماتيّة كوسيلة اتصال، وأداة معرفيّة تثقيفيّة وتعليميّة جديدة؛ لكنّها جاءت مصحوبة بأشكال مستحدثة من الجرائم التّقنيّة نسبة للآلة المستعملة في ارتكابها؛ هي الكمبيوتر الّتي صوّبت في مواجهة الإنسان والدّول؛ لزعزعة أمنها واستقرارها. طالما أنّ الشابكة هي فضاء معلوماتي حر ومفتوح لا يعرف للحدود معنى؛ لذلك يواجه الأمن المعلوماتي مجموعة من الأخطار قد تكون طبيعة هذه الأخطار أو المهدّدات مقصودة، كسرقة المعلومات أو إدخال الفيروسات من مصادر داخل أو خارج المنظّمة، أو أنّها غير مقصودة كالأخطاء البشريّة أو الكوارث الطبيعيّة، والّتي تُصنّف في شكل فئات عدّة. كما تواجه أنظمة المعلومات بعض المشاكل المعاصرة وهي تلك الشّائعة التي تساهم في تدميرها وسرقة المخزون المعلوماتي للحواسيب من فيروسات وقرصنة المعلومات وغيرها.

يعرف الأمن في اللّغة بأنّه نقيض الخوف يقول تعالى في سورة قريش الآية 04 بعد بسم اللّه الرّحمن الرّحيم أَعُوذُ بِٱللَّهِ مِنَ ٱلشَّيۡطَٰنِ ٱلرَّجِيمِ ﴿ ٱلَّذِيٓ أَطۡعَمَهُم مِّن جُوعٖ وَءَامَنَهُم مِّنۡ خَوۡفِۭ ﴾ والأمن في الإسلام لا يقتصر على النّواحي الماديّة، وإنّما يتجاوزها ليشمل الدّين، النّفس، والعقل، والعرض، والمال فحسب سلم أولويات

الحاجات الضّروريّة لدى علماء النّفس والاجتماع يقع الأمن في المرتبة الثّانيّة ليشمل: الأمن الشّخصي، والأمن الوظيفي، والأمن الاقتصادي، والأمن الاجتماعي والأمن العسكري، ويتّسع هذا المفهوم ليشمل **الأمن المعلوماتي** كـــأحد أهم المجلات الأمنيّة الّتي تتطلّبها الأفراد والمجتمعات في العصر الحديث.

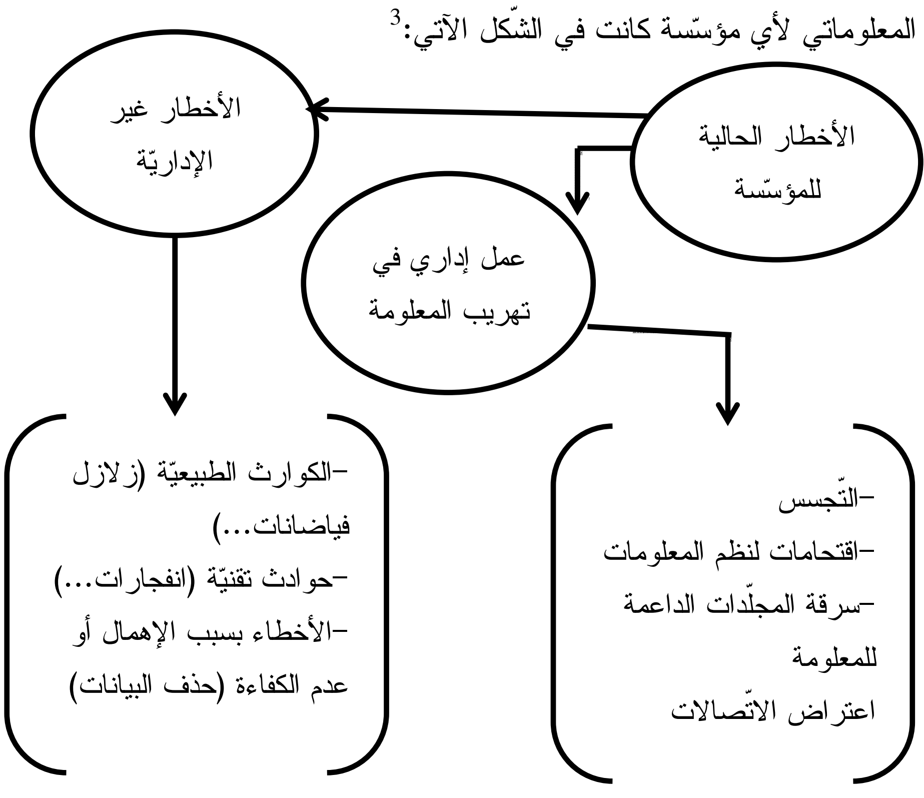
يشهد العالم منذ منتصف القرن العشرين ثورة جديدة اصطلح على تسميّتها بالثّورة المعلوماتيّة وذلك للدّور البارز الّذي أصبحت تلعبه المعلومات في الوقت الرّاهن، والّتي تشكّل البيئة التّحتيّة في أداء المهام؛ لتبقى نوع هذه المعلومات وكميّتها، وطريقة عرضها الأساس في نجاح عمليّة صنع القرارات داخل المؤسّسات المعاصرة، وعليه فإنّ للمعلومات قيمة عليها يستوجب وضع الضّوابط اللاّزمة لاستخدامها، وتداولها ووضع السّبل الكفيلة بحيازتها؛ لذا فإنّ المشكلة الّتي يجب أخذها بالحسبان هو توفير الحماية اللاّزمة للمعلومات، وإبعادها عن الاستخدام الغير المشروع لهـــا، والّذي يتحـــدد في معنـــى الأمن المعلوماتـــي (information Security)، ولقد انتشرت مؤخرا ظاهرة خبيثة تمثّلت في ما يسمى **بالجريمة المعلوماتيّة** بالرّغم من أنّ هذه الأخيرة (المعلوماتيّة) هي سمة العصر ومقياس يحدّد مدى تقدّم الشّعوب والدّول من أجل ضمان نهضتها، وتماشيا مع عصر المعلوماتيّة بأن تعمل على مواكبة التّطور التّكنولوجي الّذي نجم عنه تحوّل العديد من الدّول لمجتمعات إلكترونيّة تعتمد الرّقمنة في أعمالها مما نجم عن هذه الثّروة آثار سلبيّة أثّرت على حقوق الأفراد وحرّياتهم، نتيجة استغلالهم كوجهات تقنيّة أخرى في المعلوماتيّة في غير غرضها الحقيقي، فأضحى ما سمي بالاعتداء وإساءة الاستخدام، مما ترتّب من ذلك الإحاطة بهذه الظواهر الكثير من الغموض؛ ليصبح موضوع جرائم المساس بالأنظمة المعلوماتيّة من المواضيع الهامة والجديدة، والمعاصرة الّتي باتت الحاجة إلى دراستها بتأن واجب بالفعل كونه موضوع يتّسم بالمرونة، والتّطور الهائل في شتى الميادين، فإذا كان الكمبيوتر الدّليل المستخدم في ارتكاب الجريمة المعلوماتيّة، فمنطقي جدا أن يكون كمحل

ووسيلة لارتكابها؛ لذا تسعى الكثير من المؤسّسات في ظل تهديدات ومخاطر أمن أنظمة المعلومات؛ لإيجاد السّبل والوسائل الوقائيّة والإجرائيّة الّتي تمكّنها من مواجهة التّهديدات الأمنيّة، ولكي تتمكّن من القيام أيضا بوظائف أمنها، ويتزايد الاهتمام بالحماية سعيا للتّقليل من هذه الأخطار بعد الكشف عنها والتّنقيب فيها؛ لذا سنحاول في موضوع بحثنا هذا الإجابة عن الإشكاليّة التّاليّة: **ما هي مجموع الأخطار والمشاكل المعاصرة الّتي يمكن أن تواجهها الأنظمة المعلوماتيّة المعتمدة على الكمبيوتر؟**

تعد الولايات المتّحدة الأمريكيّة مهد المجتمع الإلكتروني كونها أوّل بلد إلكتروني في العالم لحد أن وصفت (بالجمهوريّة الإلكترونيّة)، ويعتبر العديد من الباحثين في الإعلام الآلي سنة 1980م هي سنة الميلاد الحقيقي للمعلوماتيّة (الإنترنيت)، هذه الشابكة الّتي وُلدت بعد تمخّض وبحث علمي مكثّف دام أكثر من عشرين عاما، وابتداء من عام 1981م بدأت الولايات المتّحدة الأمريكيّة تحضّر حروب الجيل الثالث، جيل الإعلام، والمعلومات، والذّكاء الإنساني، هي حروب تتلاءم مع حيثيات المجتمع الجديد.

أصبحت إدارة أمن أنظمة المعلومات قضيّة حاسمة بالفعل لأي منظّمة كانت في عصر المعلوماتيّة وكأي عمليّة أخرى، فلا يمكن إدارة أمن المعلومات من غير مقياس قابل للقياس؛ ليعد هذا الموضوع مهم في الوقت الّذي تكون فيه المنظّمات تحت ضغوط معقّدة تتطلّب المثابرة لحماية أصول بياناتهم المهمّة، فالمقياس المسمى بـــ: (نظام التّنبيه وتسجيل المخاطر) والّذي يرمز له بـــ: (CVSS) يعني: (Common vulnerabilityScoring System)[1] سيؤهّل المنظّمات للتّعرّف مسبقا على التّهديدات، ونقاط الضّعف والمخاطر الموجودة لديهم على مستوى أجهزتهم الآليّة، وبالتّالي يتجسّد مفهوم الأمن المعلوماتي في: "مجموعة من الوسائل أو الإمكانيات النّشطة والدّفاعيّة لضمان حماية التّراث المعلوماتي للمؤسّسة ونشاطاتها"[2] أي هو الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من

مخاطر الضّياع والتّلف، أو من مخاطر الاستخدام غير الصّحيح سواء المتعمّد أو العفوي، أو من مخاطر الكوارث الطبيعيّة، وسنلخّص أهم الأخطار الّتي تهدّد الأمن المعلوماتي لأي مؤسّسة كانت في الشّكل الآتي:[3]



أوّلا: التّعريف بجرائم الكمبيوتر والإنترنيت:

1- جرائم الكمبيوتر: إنّ هذا المفهوم مستحدث جدا على الصّعيد العالمي بالرّغم من أنّ أوّل حادثة موثقة بإساءة استخدام هذا الجهاز ترجع لزمن بعيد نوعا ما؛ أي لعام 1959م، وإنّ التّشريعات الّتي وضعتها الجزائر تأخّرت حتى أواخر السّبعينيات ومطلع الثّمانينيات، وكما وصفت أنّها موجة تشريع ثانيّة لتقنيّة المعلومات. بقيت إذن في حدود ضيّقة، وفي إطار عدد محدود من الدّول؛ لتمتد هذه الجرائم لتغطي: السّرقة، الاختلاس، التّزوير، الاحتيال، الإتلاف والتّدمير، الافتراء تعطيل الخدمة، الاستغلال غير المشروع للمال، الإضرار بمال الغير...الخ،[4]ومن

الأفعال الّتي ربما تصل لحد القتل. يلعب الكمبيوتر ثلاثة أدوار في ميدان ارتكاب الجرائم، وكذا دورا رئيسيا في حقل اكتشافها، ففي حقل ارتكاب الجرائم يكون للكمبيوتر الأدوار التّاليّة:[5]

الدّور الأوّل: قد يكون الكمبيوتر هدفا للجريمة (Target of anoffense) وذلك كما في حالة الدّخول غير المصرّح به إلى النّظام، أو زراعة الفيروسات لتدمير المعطيات والملفات المخزّنة، أو تعديلها، وكما في حالة الاستلاء على البيانات المخزّنة أو المنقولة عبر الأنظمة.

الدّور الثّاني: وقد يكون الكمبيوتر أداة الجريمة لارتكاب جرائم تقليديّة (Atoolin the commission traditionnel offense)، كما في حالة استغلال الكمبيوتر للاستلاء على الأموال بإجراء تحويلات غير مشروعة، أو استخدام التّقنيّة في عمليات التّزييف والتّزوير، أو استخدام التّقنيّة في الاستلاء على أرقام بطاقات ائتمان، وإعادة استخدامها والاستلاء على الأموال بواسطة ذلك.

الدّور الثّالث: وقد يكون الكمبيوتر بيئة الجريمة، وذلك كما في تخزين البرامج المقرصنة فيه، أو في حالة استخدامه لنشر المواد غير القانونيّة، أو استخدامه أداة تخزين، أو اتّصال لصفقات ترويج المخدّرات وأنشطة الشابكات الإباحيّة ونحوها وطبعا يمكن للكمبيوتر أن يلعب الأدوار الثّلاثة معا، وفي آن واحد.

تمثّل إذن هذه الجرائم تحدّيا كبيرا لإدارة أنظمة المعلومات؛ لما تسبّبه من خسارة كبيرة من خلال الاستخدام والوصول، والتّعديل، والتّدمير غير المفوّض للماديات والبرمجيات، أو البيانات، وموارد الشابكة فضلا عن النّشر والنّسخ غير المفوض للمعلومات، وحرمان المستفيد النّهائي من الوصول لمادياته وبرمجياته، أو بياناته، فقد تكون جريمة الكمبيوتر بريئة نسبيا مثل الاستخدام غير المفوّض للحاسبات لأغراض شخصيّة، أو تكون خطيرة كاستخدام الحاسبات لإرسال موجودات المنظّمة الحاليّة لحساب منظّمات أخرى. هكذا إذن تفاقمت المعلومات لتصير أكثر الأشياء تأثيرا إما على المستوى الوطني، أو الشّخصي، أو الدّولي إذ

لها آثار عميقة وكبيرة في التّطور والتّنميّة في القطاعات المختلفة، ولما لها من دور في تنظيم الحياة والعلاقات بين الأفراد والمؤسّسات العامة والخاصة؛ لذا وجب التّعامل معها بمستوى عال من الوعي، من أجل أن تؤدي هذه المعلومات دورها الفعال في تحقيق الأمن، والعدالة، والحياة الكريمة للجميع بحيث نعلم أنّ الشابكة بدورها لم تعد مجرّد أداة إيجابيّة للحصول على المعلومات بل أصبحت تشكّل خطورة كبيرة على المستخدمين، وتنجم المشكلات الأمنيّة في أنظمة المعلومات المنقولة من الشابكة بسبب:[6]

- عدم التّواجد الفعلى؛ أي أنّ التّواجد إفتراضي؛
- سهولة النّسخ، والتّعديل للمعلومات؛
- إحداث أنشطة آليّة تعمل عبر برامج، وبعضها يضر بالأنظمة؛
- إمكانيّة الدّخول للمعلومات من أي جهة كانت، وفي أي وقت كان؛ أي شيوع التّواجد.

2- جرائم الإنترنيت: تمر أنظمة المعلومات عبر الشابكة بدورة حياة شبيهة بدورة حياة الإنسان؛ أي أنّها تمر بمراحل مترابطة، ومتداخلة والّتي تحتاج لعمليّة تطوير وبذل جهود مستمرّة. فيها يتمّ تحديد الفجوة الملحقة بهذه المعلومات والتّغلب عليها من أجل التّوصّل لإنجازات تستفيد من استخدام واستثمار التّكنولوجيا داخل المنظّمات، وبخاصة ما يتعلّق بأنظمة المعلومات الإداريّة؛ كونها طريقة ذات طابع هيكلي منظّم، والّتي تتكوّن من مراحل أساسيّة مترابطة ومتكاملة، والشّكل التّالي يمثّل نموذج تدفّق دورة حياة أنظمة أمن المعلومات.[7]

شكل يوضّح مراحل تدفق دورة حياة أنظمة المعلومات



نلاحظ من خلال الشّكل أنّه يسير في اتّجاه دوراني مستمر؛ ليمثّل عمليات التّقييم، وذلك حتى يتمكّن مطوّريها معرفة مواطن الخلل وإصلاحها، وتبقى جرائم الإنترنيت لها خصائص تجعل من الصّعوبة بمكان التّصدي لها وهي:[8]

- جريمة لا تترك أثرا بعد ارتكابها؛
- صعوبة الاحتفاظ الفني بآثارها إن وجدت؛
- تحتاج إلى خبرة فنّية، ويصعب على المحقّق التّقليدي التّعامل معها؛
- تعتمد على الخداع في ارتكابها، والتّظليل في التّعرّف على مرتكبيها؛
- تعتمد على قمّة الذّكاء في ارتكابها؛
- ترتكب في دولة ما، ويتحقق الفعل الإجرامي في دولة أخرى.

إنّ كوارث الكمبيوتر والشابكة تشكّل عامة تأثير كبير على تكنولوجيا المعلومات، والّتي بدورها تؤثّر على فاعليّة، وربحيّة، ومنافسة شديدة في ما بين الشّركات تشمل: فيروسات، قرصنة المعلومات، أخطاء الأجهزة، التّخريب، مشاكل البرامج، الإهمال البشري، والكوارث الطبيعيّة...الخ، ونحن من الصّعب جدا الإلمام، والتّفصيل فيها ككل؛ لذا سنحاول التّفصيل في ما يسمى بالفيروسات وقرصنة المعلومات.

ثانيا: الفيروسات (VIRUS)

تعود ظاهرة فيروسات الكمبيوتر إلى نهاية الأربعينيات، وقد ورد ذكرها لأوّل مرّة في مقال نشره (جون فون نيونان) سنة 1949م، وظهرت بعدها بعض عوارض الفيروس في أوائل الخمسينيات؛ لكّنها في هذه المرحلة بقيت محدودة جدا وكان أوّل انتشار للفيروسات على مستوى أجهزة الشابكة عام 1983م، إذ ظهرت بالضّبط مع نظام التّشغيل(Unix)، بحيث أثارت ضجّة في السّاحة العلميّة والعمليّة ولم تسلم أكبر الشّركات من هذه الفيروسات، وتنتشر اليوم انتشارا مولعا؛ لتصبح خطر يهدّد الاقتصاد، والحكومات والأفراد، فشبّهها البعض في عهد الإنترنيت هذا وكأنّها منحت الأسماك ببحيرة من الماء ترتع فيها وتتكاثر، إذ تنتشر في أكبر عدد من الأجهزة وفي أقلّ فترة زمنيّة ممكنة،[9] فهي إذن من أكثر جرائم الكمبيوتر إمعانا في الشّر.

1- تسمية الفيروس: لم تكن هذه التّسميّة بالفيروس عبثا أو صدفة بل ثمّة نقاط مشتركة ما بين الفيروس البيولوجي، والفيروس المعلوماتي، وبالتّالي الفيروس سواء كان معلوماتيا، أو بيولوجيا يبقى مسؤول على التّشويش في نقل المعلومة ففيما يتعلّق بالفيروس البيولوجي، فإنّه ينقل معلومات الخلايا الوراثيّة، وهو ما يؤدي إلى نسخ طبعة الأصل من الخليّة (النواة المعلوماتيّة) المصابة ممّا يؤدي إلى إصابة الجسم كلّه، وتتعدّد أنواع الفيروسات في مجالين مختلفين، وفي كلا الحالتين هناك أنواع متشابهة في الخطورة أو في طريقة التّكوين، كما تتشابه أيضا في طريقة التّكاثر.[10]سنتطرق الآن لمفهوم الفيروسات في الأنظمة المعلوماتيّة.

2- مفهوم الفيروسات: تعتبر الفيروسات من أهم جرائم الكمبيوتر، وأكثرها انتشارا في الوقت الحاضر ويمكن تعريفها بأنّها: برنامج حاسوب له أهداف تدميريّة، يهدف إلى إحداث أضرار جسيمة بنظام الحاسوب سواء البرامج أو الأجهزة، ويستطيع أن يعدّل تركيب البرامج الأخرى حيث يرتبط بها ويعمل على تخريبها، وهو برنامج مكتوب بإحدى لغات البرمجة من قبل المبرمجين، وهو قادر

على التّوالد والتّناسخ، ويستطيع الدّخول إلى البرامج، له الأفضليّة أكبر من نظام التّشغيل في فحص المكوّنات الماديّة مثل: الذاكرة الرئيسيّة، أو القرص المرن، أو اللّيزري.[11] في تعريف آخر للفيروسات حسب (Hyatt) يقول: "أي برنامج أو مجموعة من التّعليمات قد تلحق ضررا بنظام المعلومات، أو ما يحتويه من معلومات، ولديها القدرة على التّخفي، والتّوسع، والانتشار"[12] ولاشك من وجود جملة عوامل مساعدة على انتشار الفيروسات.

3- عوامل انتشار الفيروسات: هناك مجموعة عوامل تسهم في خطورة الفيروسات وانتشارها وهي:[13]

- **انتشار الشابكات:** بحيث تزداد الهجمات في بيئة الإنترنيت؛ ليحدث ذلك آليا دون تدخّل من البشر.
- **زيادة تعقيد الأنظمة:** حيث تزداد الثّغرات الّتي من الممكن أن تشكّل أداة لتفاقم المشكلة الأمنيّة.
- **سهولة الإضافة إلى الأنّظمة:** بحيث إنّ الإضافات (Addplugin) وأدوات التّوسعة (Extension systems) وما يطلق عليه (Scripts) تقوم بدور بارز في إنهاك الأنظمة الأصليّة.

4- أنواع الفيروسات: ينفرد متخصّصوا تقنيات المعلومات في التّفريق بين الأنواع المختلفة من الفيروسات، بحيث لا يميّز الكثير من النّاس بين الفيروسات وغيرها، مما يُعرض الكمبيوتر للخطر كالدّيدان، وأحصنة طروادة وغير ذلك، وتحمل هذه الأخيرة تحت عنوان أشمل هو: **البرمجيات الضارة (Malicious software)**، إذ تعمل على تقليص أداء موارد الأنظمة، وقد عرفت هذه البرامج بأنّها البرامج الّتي تُضمن أو تُدخل عمدا إلى نظام ما ولغرض ما ضار وتشمل ما يلي:

4. 1-الدّيدان: وهي برامج حاسوبيّة مستقلّة بذاتها تجد ضالتها في الانتشار عبر أجهزة الشابكة المحليّة.

4. 2- أحصنة طروادة (Trojans): وهي برامج تبدو عاديّة لكّنها تحمل في جوانبها الخطر غير المتوقّع بما تقدّمه من ضرر خفي، وسميّت بهذا الاسم نسبة إلى القصّة التّاريخيّة الشهيرة لخداعة حصان طروادة الخشبي الشهير في الأدب الإغريقي جنود اسبرطة للاختفاء في خوفه بعد أن تظاهروا بالانسحاب، فقام أهل طروادة بسحب الحصان إلى داخل المدينة المنيعة الّتي استعصت على الهجوم حتّى أن هدأت المدينة، وبعد نوم الحراس خرج الجنود المختبئين من الحصان الخشبي وفتحوا أسوار المدينة، وبعدها تدفّق جنود الأعداء إلى المدينة واستولوا عليها. عرف هذا الفيروس أيضا بـــ: "عبارة عن برنامج صحيح، وقانوني لإجراء عمل مفيد، ولكن ضمنه تنفذ شفرات مختفيّة، والّتي قد تكون فيروس يسمح بوصول غير مخوّل للكمبيوتر بهدف تدمير البيانات والملفات"[14] ومن أمثلة هذه البرامج الضارة: ما يسمى بالقنابل الموقوتة، باب المصيدة، وكلّها تهدف لتجاوز أنظمة الحماية لأمن المعلومات.

4. 3- برامج التّجسس: هي برمجيات تقوم بجمع المعلومات الشّخصيّة بدون معرفة النّاس وإذنهم بعدها تقوم بإرسال المعلومة إلى طرف ثالث (أشخاص، أو شركات، أو خادمات (Servese)...الخ) وهذه المعلومات قد تكون حرجة تسبب الخسائر، أو تتعرّض لسوء الاستخدام منها مثلا: البرمجيات المساعدة (Adware) برمجيات التّلويث (Malware)، الاستخدام (Evalware)، وهي تختلف عن الدّيدان والفيروسات كونها لا تنسخ نفسها، فتشتغل برمجيات التّجسس على الثّغرات الأمنيّة لأنظمة التّشغيل، وبرامج اعتراض الإنترنيت لأغراض تجاريّة، أو تخريبيّة، أو لأجل بيع المعلومات لمؤسّسات إعلانات، أو شركات عن طريق سرقة المعلومات الشّخصيّة للمستخدم، ومراقبة نشاطه أثناء تصفّح شابكة الويب.[15]

4. 4- مسجلات ضربات المفاتيح: وهي برمجيات صغيرة تقوم بتسجيل ضربات المفاتيح الّتي يقوم بها المستخدم سعيا لالتقاط كلمات المرور وتخزينها وكذا المعلومات الخاصة أيضا، كأرقام بطاقات الائتمان، وبعض هذه البرمجيات

لها أهداف حميدة لما يقوم المستخدم بتثبيته من أجل الحماية الأسريّة وبخاصة في حالة استخدام الأطفال للإنترنيت، وخوفا عليهم من استغلالهم من قبل مواقع ذات أغراض سيّئة.[16]

4. 5- الفيروس التّقليدي: يقوم بتخريب وسائط كالأقراص الخارجيّة والقرص الصّلب، ويكون مسكنّه إمّا في منطقة النّظام، أو ملفات البرامج، أكثر أنواع الملفات قادرة على حمل الفيروسات، لكن أغلبها يكون من نوع ملفات التّنفيذ (exe)،[17] وأنّ ملفات التّنفيذ لا تبدأ عملها إلّا عندما يتم فتحها من قبل مستخدم الجهاز.

4. 6- فيروس الماكرو: يعني الماكرو في علم الكمبيوتر مجموعة من الأوامر يتم تسجيلها ببرامج مثل: (فيجوال بيسك) لتعطي وظيفة صغيرة في برنامج مثل: (مايكروسوفت وورد) يستغل البعض هذه الخدمة لكتابة الفيروسات الّتي تلوّث ملفات البيانات المنشأة ببرامج مثل برنامج مايكروسوفت وورد، أو أكسل، أو أكسس، أو باوربوينت.[18]علما أنّ هذا الفيروس أحدث من الفيروس التّقليدي وحوادثه في تصاعد كبير، لكنّه لا يبدأ عمله الضّار إلا عند فتح ملف يحوي ذلك الماكرو.

4. 7- فيروس باب المصيدة: عبارة عن رمز يتم توزيعه عند تركيب باب الحماية؛ لكي يعطي المخرّب حرّية اختيار الوقت المناسب لعمليّة التّخريب، بحيث يسمح هذا الرّمز بالنّفاذ من خلال الشابكات في وجود أنظمة الحماية الّتي تعتاد على وجوده.[19] كما سبق وأن أشرنا بأنّ هذا الفيروس ينتمي لأحصنة طروادة.

4. 8- فيروسات العتاد: تصمم في أصلها لتصيب العتاد حيث يبرمج هذا الفيروس، لتنفيذ ملايين العمليات الحسابيّة المتواليّة دون استخدام أوامر للإخراج أو الإدخال، ومن ثمّ يلقى عبئا كبيرا على وحدة المعالجة المركزيّة،[20] فيؤدي لارتفاع درجة حرارتها وفسادها واحتراقها.

4. 9- فيروس البلوتوث: إنّ نشر الفيروسات عن طريق البلوتوث حازت على مرتبة معتبرة كونها الطريقة السّهلة والسريعة في الآن نفسه، والّتي تعتمد على ربط وتوصيل الأجهزة الإلكترونيّة المحمولة كالكمبيوتر والحاسب الجيبي، أو الهاتف المتحرّك، ونقل الملفات بينها، وبين الشابكة لا سلكيا، وهي أطور وسائل نقل المعلومات من جهاز لآخر. مما جعل إمكانيّة انتقال الفيروس من جهاز لآخر عبر البلوتوث عمليّة ممكنّة الحدوث، وذلك بأن يقوم الجاني بإرسال فيروس من جهازه إلى جهاز آخر ويؤدي ذلك إلى تلف وتعطيل هذا الأخير (المرسل إليه) فيحدث في الحين إضعاف البطاريّة، وتكرار غلق الجهاز تلقائيا.[21] يبقى فيروس الكمبيوتر كبرنامج غير عادي مستنسخ لنفسه صمم أصلا للانتشار من جهاز لآخر يمكن له أن يخرّب، أو يمسح البيانات من الجهاز كما يمكنه استخدام البريد الإلكتروني للانتشار، أو حتى مسح كل شيء بجهازك، ويكثر الانتشار عادة عبر مرفقات البريد الإلكتروني؛ لذا من المهم جدا أن لا تفتح أي مرفق بالبريد إلاّ إذا كنت تعرف المرسل.

تستهدف الفيروسات عادة البرامج التّنفيذيّـة، والّتي تنتهـي مسمّياتهـا بالتّرميز التّالي: com, .vbx, .lin, .sys, .dre, .dll, .exe,.ovl. وكذا البرامج التّحميليّة منها مثلا جدول تقسيم الأسطوانة الصلبة (Partition table)، وسجل التّشغيل (Boot record)، وسجل التّشغيل الرّئيسي (Mastor boot) وجدول فهرس الملفات (FAT)؛[22] لتبقى بعض الاعتقادات العالقة والخاطئة عن الفيروسات شائعة بين غالبيّة المستخدمين منها: أنّ الفيروسات لا تنتشر باستخدام ملفات البيانات، وأنّ قراءة البريد الإلكتروني لا يمكن أن تسبب بإصابة الجهاز بالفيروس، أو أنّ الفيروسات لا يمكن أن تسبب تلف في قطع الحاسب، وأنّ فيروسات البرامج التّحميليّة هي الأكثر خطرا، أو أنّ الفيروسات لا تعمل جيّدا في بيئة النّوافذ...الخ ونحن نقول وننصح بالحيطة والحذر؛ لأنّها خطيرة وأضرارها وخيمة على الأنظمة المعلوماتيّة بصفة عامة، وتقوم بأعمال عديدة حسب رغبة مصمّميها من ذلك نجد:

- تدمير البيانات وبرامج التّشغيل؛
- تشغيل برامج غير مطلوبة؛
- إبطاء سرعة عمل الجهاز.

5- **طرق العدوى بالفيروسات:** هناك ثلاث طرق رئيسيّة وهي:[23]

- وسائط التّخزين الخارجيّة؛
- تنزيلات الإنترنيت؛
- مرفقات البريد الإلكتروني.

6- **أعراض إصابة الكمبيوتر بالفيروسات:** عديدة وهي:[24]

- التّكرار في ظهور رسائل الخطأ في أكثر من برنامج؛
- توقف بعض البرامج عن الاستجابة؛
- حدوث بطئ شديد في إقلاع برامج التّشغيل، أو عند تنفيذ بعض التّطبيقات؛
- مشاكل في العرض على شاشة الكمبيوتر؛
- توقف الأنظمة عن العمل؛
- مسح الملفات وتدميرها؛
- ظهور ضوء غير مألوف في مشغل الأقراص؛
- تخريب القرص الصّلب.

إنّ التّطورات الحاصلة في مجال إعداد برامج الفيروسات جعلت من الصّعوبة بمكان إيجاد طريقة مضمونة بدرجة كبيرة للوقاية من الفيروسات، ولكن هناك بعض الأساليب الفّعالة الّتي يمكن اتّباعها للحماية منها:[25]

- تركيب برنامج مضاد للفيروسات ملائم لنظام التّشغيل المستخدم في جهاز الكمبيوتر، ويفضّل أن يكون نسخة أصليّة للاستفادة من الدّعم الفني للشّركاء الّتي يتم شراء البرامج المضادة منها؛
- عدم وضع برنامج جديد على جهاز الكمبيوتر، إلا قبل اختباره، والتّأكد من خلوّه من الفيروسات بواسطة برنامج مضاد للفيروسات؛

- عدم استقبال أيّة ملفات من أفراد مجهولي الهوّية على الإنترنيت؛
- عمل نسخ احتياطية من الملفات الهامة، وحفظها في مكان آمن؛
- التّأكد من نظافة أقراص اللّيزر الّتي يُحمل منها نظام التّشغيل الخاص بجهاز الكمبيوتر؛
- حمل البرامج من مواقع تثق بها فقط، ومع ذلك قم بفحصها قبل فتحها؛
- تأكد من تحديث البرامج المضادة للفيروسات باستمرار؛
- تأكد من تفعيل خاصيّة تحديث برنامج التّشغيل أليا لسد الثّغرات الأمنيّة وكذلك بقيّة البرامج الهامة مثل برنامج مايكروسوفت أوفيس؛
- إذا اعتقدت بأنّ الكمبيوتر قد أصيب بفيروس، ولاحظت أيا من العوارض المذكورة قم مباشرة بحمل فحص شامل بمضاد الفيروسات؛
- إيقاف التّحميل من مشغل الأسطوانات المرنة؛
- متابعة وتركيب جميع التّعديلات والإصلاحات الموفّرة من مصنعي البرامج، وبخاصة نظم التّشغيل؛
- مسح جميع ملحقات البريد الإلكتروني؛
- تحديث برنامج المتصفّح أوّلا بأوّل.

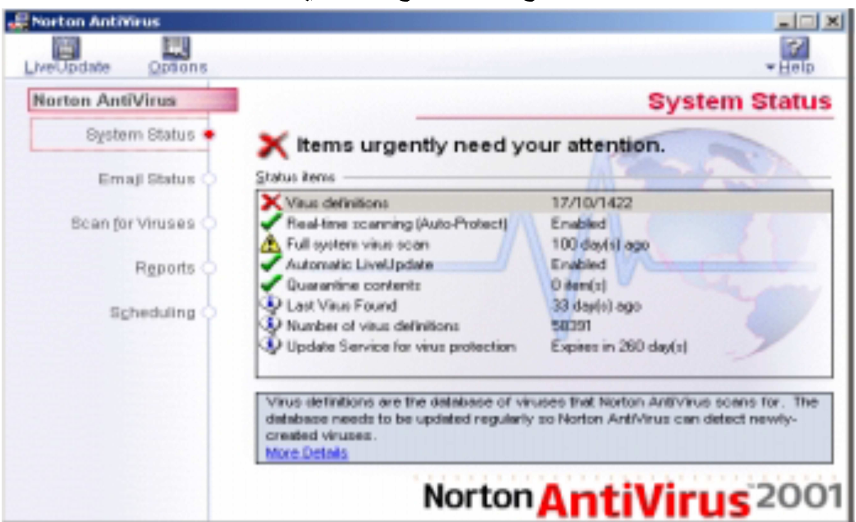
7- **برامج الحماية من الفيروسات:** هي برامج تركب، ويُثبت لها مساعدات في جميع الحاسبات الأعضاء في الشابكة، ويتمّ تحديث الحادث يوميا من الشّركة الصّانعة، وكما يتمّ تحديث المساعدات من خلال الخادم داخل الشّابكة تبعا للسّياسة الأمنيّة الموضوعة في المؤسّسة، كما يتم تنفيذ فحص دوري يومي غالبا لجميع الحاسبات من أمثلتها مثلا نجد: (Trend Mictoofice scan)، (Avir-Antivir) (Sophos)، (Norton)، (E-trust)، (Mac Afee)، (KasperSky)، (Avact)،[26] ونشير إلى هذه البرامج في الشّكل الــتالي:

شكل يوضّح أنواع برامج الحماية من الفيروس



تعتبر برامج مسح الفيروسات هذه كأدوات في غاية الأهميّة، لضمان أمن المراسلات عبر الإنترنيت يجب الحرص على تنصيبها، وأن يكون مصدرها موثوق؛ لأن ما يحدث في البعض من البلدان يتم بيع نسخ مقرصنة من هذه البرامج في الشوارع، أو يتم تنصيبها في المتاجر الّتي تبيع أجهزة الكمبيوتر، ولذا يجب العلم بأنّ هذه المصادر غير آمنة؛ لأنّ هناك طرفا ثالثا من الممكن لأن يكون قد غيّر محتوى البرنامج لخدمة غاياته الخبيثة. كما أنّ البعض من هذه البرامج متوفّرة بالمجان يمكن تحميله أو نسخه من الشابكة، مثل برنامج (Avira)؛ لمسح الفيروسات، ويمكن أيضا النّفاذ إلى الموقع، وتحديثات البرنامج في البلدان الّتي تخضع لحظر تصدير من قبل الدّول الغربيّة، يمكن إذن تحميل نسخة (Avira) من الموقع التّالي: http://www.avira.com/en/avira-free-antivirus[27] وسنبيّن في ما يلي أحد برامج التّصدي للفيروسات.

شكل يوضّح أحد برامج التّصدي للفيروسات



تبقى برامج مكافحة الفيروسات برامج مصمّمة، لاتخاذ جميع الاحتياطات اللاّزمة لحماية أجهزة الكمبيوتر من الفيروسات، وهي من أهم وسائل الحماية تقوم بمنع دخول الفيروسات على مستوى الأنظمة واكتشافها فظلا عن قيامها بتحديث نفسها بشكل آلي عن طريق الإنترنيت؛ لتزيد من قدرتها وكفاءتها على مكافحة الفيروسات. هذه إذن بعض الأساليب الجديدة من شأنها أن تساهم في ضمان حماية أجهزة الكمبيوتر، ولكن يجب أن نضع نصب أعيننا، ولا نتصور أنّ وجود برنامج مضاد للفيروسات محدث دائما في أجهزة الكمبيوتر يعني أنّنا في مؤمن من الفيروسات. كما أنّ أية مشكلة في الأجهزة لا تعني دائما أنّ هناك فيروسا؛ لذا يجب تحديد سبب المشكلة، ومحاولة إيجاد العلاج لها.

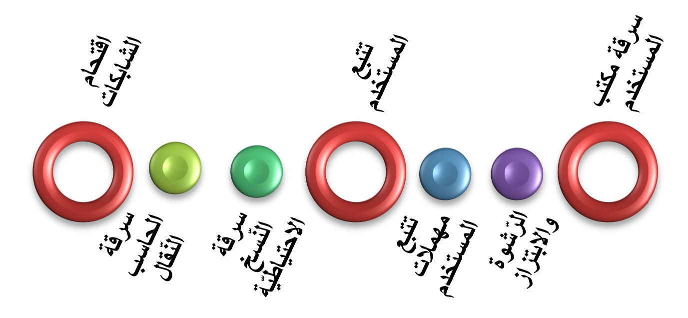
إنّ البرمجيات المضادة للفيروسات تقوم بعمل رائع في كشف، ورصد، وإزالة الفيروسات الكامنة في الأقراص المرنة، والضّوئيّة، والذّاكرات (الفلاش)، وانتقال هذه الفيروسات بطيء نسبيا بالنّسبة لنشرها من خلال الإنترنيت والبريد الإلكتروني.

ثالثا: القرصنة المعلوماتيّة

يسمع الكثير بما يسمى (الهاكرز) أو مخترق الأجهزة (Hackers)، ونتساءل كيف يتم ذلك؟ وهل الأمر بسيط لهذا الحد؟ أم أنّه يحتاج لدراسة وجهد ففي الحقيقة ومع انتشار برامج القرصنة، ووجودها في الكثير من المواقع أصبح من الممكن اختراق أي جهاز كمبيوتر، وبدون عناء فور إنزال إحدى برامج القرصنة والمقصود بها هو: سرقة المعلومات من برامج وبيانات بصورة غير شرعيّة، وهي مخزّنة في ذاكرة الكمبيوتر، أو نسخ برامج معلوماتيّة بصورة غير قانونيّة، وتتمّ هذه العمليّة بعدّة طرق إما بالحصول على كلمة السّر، أو بواسطة التقاط موجات كهرو مغناطسيّة بحاسبة خاصة، ويمكن إجراء عمليّة القرصنة بواسطة رشوة العاملين في المنظّمات المنافسة.[28] أوّل قرصان معلوماتي في التّاريخ هو شخص حفر في منطقة نائيّة على خط هاتف يصل بين مؤسّستين عسكريتين، ثمّ وصله على هاتفه، وتنصّت على المحادثات.[29] أما اليوم ومع التّطور التّكنولوجي، وكون الجميع موصولا على الإنترنيت، فالقراصنة ليسوا بحاجة إلى الحفر إذ يمكنهم وهم جالسين خلف أجهزتهم الخاصة اختراق جهازك، وسرقة الملفات المخزّنة عليه، أو وصل أنفسهم افتراضيا على خطّك ومراقبتك، ومراقبة اتّصالاتك على الشّابكة.

تعود أحد أشهر قضايا الاختراق لنهاية الثّمانينيات من طرف مجموعة من المراهقين الألمان الّذين تمكّنوا من الدّخول إلى أنظمة العديد من الشّركات الأمريكيّة، وجمع معلوماتها بقصد بيعها إلى المخابرات السّوفياتيّة سابقا، وقد اكتشفت هذه القضيّة عن طريق تعاون أحد (الهاكرز) مع جهات التّحقيق بحيث قدّم لها كافة معلوماته بشأن كيفيّة حدوث الاختراقات والأنظمة المستهدفة، وكانت هذه الأخيرة أكثر القضايا أهمّية بالنّسبة لجهات التّحقيق في ما بعد لما كشفته من تفاصيل عن الآليات التّقنيّة، والوسائل الّتي استخدمها هؤلاء في الحصول على المعلومات.[30] يعتمد نظام الاختراق هاكنج (Hacking) بشكل أساسي على طبيعة

الاتّصال بالنّظام، ووسائل الاتّصالات المرتبطة بنظام الكمبيوتر ففي، طورها الابتدائي والتّقليدي تعتمد أنشطة (الهاكرز) على تجاوز كلمات السّر الّتي تحمي أنظمة الكمبيوتر، والّتي كانت تتم طبعا عن طريق تخمين الكلمة تبعا للشّخص المستخدم، أو المؤسّسة لاسيما أنّ أغلب كلمات السّر تكون مرتبطة بحوادث ووقائع، وأسماء مألوفة، ومتّصلة بأحد أشخاص مستخدميها (تاريخ الميلاد اسم الزّوجة اسم الصّديق أو الصّديقة، اسم المنشأة وغيرها)، وبعد مرور الوقت ومع التّطور التّكنولوجي تطوّر أسلوب الحصول على كلمات السّر عن طريق استخدام برمجيات الاحتمالات وربطه بالنّظام المنوي واختراقه، ومع شيوع استخدام الإنترنيت، والربط الواسع للشابكات المحليّة بالشابكة العالميّة تغيّرت أساليب الهاكرز، إذ أصبحوا يعتمدون على عمليات الدّخول عن طريق الشابكة واستغلال بروتوكولات الاتصالات المستخدمة فيها، أو وسائل تقصي البيانات الخاصة بالمستخدمين مثل (Web spoofing) وبعد جمعها وتحليلها، أو نسخ كلمات السّر الخاصة بهم، وكذلك عن طريق اعتراض البيانات، وانشاء أنظمة وهميّة للاستقبال والتّوجيه تلتقط الرّسائل وعناوين المواقع، وتتظاهر بأنّها الجهة المرسلة إليها؛ بل إنّهم طوّروا وسائل لتجاوز كافة إجراءات الأمن، كتجاوز جدران النّار، وفك شفرات التّشفير، وتجاوز بروتوكولات أمن البريد الإلكتروني،[31] وغير ذلك من رسائل تقنيّة، وفي المخطط التّالي نوضّح بعض وسائل سرقة المعلومات.



لقد أصبحت القرصنة المعلوماتيّة اليوم شبح يهدّد العالم، وهاجس أمني يتحدّى قيام الحكومة الإلكترونيّة، فالأمر يستدعي تأمين البيانات، والمعلومات لبعث الثّقة والأمان في تعامل بعضها البعض وبالتّالي يتلخّص مفهوم القرصنة في:

1- مفهوم القرصنة المعلوماتيّة: يشير مفهوم القرصنة الإلكترونيّة إلى استخدام وسائل الاتّصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التّحايل على أنظمة المعالجة الآليّة لكشف البيانات الحساسة (المصنّفة) أو تغييرها، والتّأثير على سلامتها، أو حتى إتلافها.[32] يقوم بعمليّة القرصنة أشخاص هواة أو محترفين وتمّ تعريفهم كالتّالي: "أشخاص لهم القدرة على التّعامل مع أنظمة الحاسب الآلي والشابكات بحيث تمون لهم القدرة على تخطي أي إجراءات، أو أنظمة حماية اتخذت لحماية تلك الحاسبات، أو الشابكات."[33] يتم تصنيف هؤلاء المخترقين لصنفين.

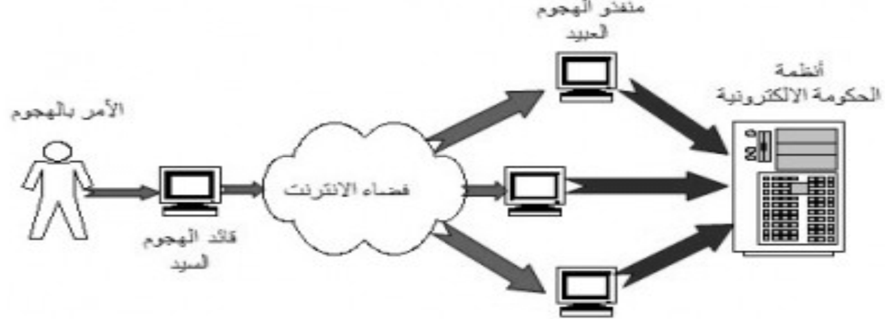
2- أصناف المخترقين:

2. 1- الهاكرز (HAKERS): هؤلاء لهم القدرة الفائقة على اختراق الأجهزة، والشابكات أيا كانت إجراءات وبرامج الحماية، الّتي تمّ اتّخاذها إلّا إنّهم لا يقومون بأي من الإجراءات الّتي تؤدي من ثمّ إلى الإضرار نتيجة في اختراق جهازه أو شابكته.

2. 2-الكراكز (CRACKERS): هؤلاء يطلق عليهم المخرّبين، وهم يتشابهون مع الهاكرز في قدرتهم الفائقة على الاختراق، وتخطي إجراءات وبرامج الحماية، إلاّ أنّهم يقومون بالعبث بالبيانات والمعلومات المخزّنة على تلك الحاسبات أو الشابكات.[34] يَعتبر الخبراء الفترة الممتدّة من 1980م إلى 1989م العصر الذّهبي للقرصنة، وتجدر الإشارة هنا إلى أنّ أشهر حروب النّت على الإطلاق هي حرب الهاكرز العظمى الّتي دارت بين عامي 1990م، و1994م بين فريقين من الهاكرز المخترقين إذ يسعى كل فريق لاختراق حواسيب الآخر. كما شهد عام 2000م حرب إلكترونيّة دوليّة من العرب المسلمين ضد اليهود، فكانت نتيجتها

اختراق وتعطيل الكثير من المواقع الإسرائيليّة وغيرها، ولعلّ أشهر القراصنة على الإطلاق هو الأمريكي (كيفن ميتنيك)، يعتبر هذا الأخير أشهر هاكر في التّاريخ هو من أطلق على نفسه (The Mentor) قام هذا الأخير بنشر دراسة شهيرة بعد أن تمّ اعتقاله أصبحت تعرف بـــ: (بيان الهاكر)[35] تكمن إذن خطورة القرصنة أكثر عندما لا تستطيع أجهزة الأمن الإلكتروني اكتشاف مصدر الاختراق أو القرصنة هو ما أطلق عليه عبارة **الهجوم السّيد**، وهو ما يوضّحه المخطط التّالي:

شكل يوضّح القرصنة الإلكترونيّة عن طريق الهجوم السّيد



يقوم هذا النّوع من الهجوم الإلكتروني المبيّن في الشّكل على مبدأ توزيع الأدوار بين البرنامج قائد الهجوم (Master Attachers)، والبرامج المنفذّة للهجوم (Slave Attachers)، إذ يقوم الشّخص الآمر بالهجوم بإعداد برنامج رئيسي يرسل إشارة الهجوم ببرامج فرعيّة موجودة على العديد من الأنظمة المربوطة بالإنترنيت، وهو أخطر هجوم إذ يظهر لوحدات الأمن الإلكتروني في الدّولة بأنّ الهجوم صادر من نقاط تواجد الأنظمة الفرعيّة في حين أنّ الهجوم الإلكتروني الفعلي يكون قد تمّ عبر البرنامج الرّئيسي، وبإشارة من الشّخص المسؤول، ولسوء الحظ لن تتمكّن أجهزة الأمن الإلكتروني من كشف المهاجم الفعلي؛[36] ليقع بعد ذلك في الفخ اتّهام أشخاص غير معنيين كلّيا بالهجوم.

3- وسائل وأساليب القرصنة: من أهمّها نجد[37]

3. 1- الفيروسات: والّتي سبق وأن فصّلنا فيها كإحدى أنواع البرامج الآليّة إلاّ أنّ الأوامر المكتوبة في هذه البرامج تقتصر على أوامر تخريبيّة ضارة بالجهاز

ومحتوياته، ويتكوّن برنامج الفيروس بشكل عام من أربعة أجزاء رئيسيّة تساهم في القرصنة المعلوماتيّة وهي:

- **آليّة التّكرار:** وهو الجزء الّذي يسمح للفيروس أن ينسخ نفسه؛
- **آليّة التّخفي:** وهو الجزء الّذي يجعل الفيروس قادرا على الاختفاء، ويمكن أن يتضمّن تشفيرا لمنع البرامج الماسحة، والّتي تبحث عن نموذج الفيروس من اكتشافه؛
- **آليّة التّنشيط:** وهو الجزء الّذي يسمح للفيروس بالانتشار قبل أن يتمكّن المستثمر من تحديد مكانه ومسحه كاستخدام توقيت السّاعة في الكمبيوتر، أو الانتظار لتنفيذ برنامج ما عددا معيّنا من المران؛
- **آلية التّنفيذ:** وهو الجزء الّذي ينفذ الفيروس عندما يتم تنشيطه ويكون مجرّد رسالة على الشاشة أو مسح بعض الملفات.

3. 2- الإغراق بالرّسائل: وذلك عن طريق البريد الإلكتروني تلك الطريقة الّتي تعني إرسال كم هائل من الرّسائل عبر البريد الإلكتروني لجهاز الكمبيوتر والمراد هو العمل على تعطيلها وتوقّفها عن العمل، وتلك الرّسائل لا تعني شيئا، قد تكون محمّلة بملفات كبيرة الحجم لمجرّد التّأثير على الجهاز ونظرا لصغر المساحة المحدّدة للبريد الإلكتروني في معظم الأحيان تصل للجهاز دفعة واحدة، وفي وقت واحد، وبالتّالي تسبب في توقّفه عن العمل على الفور لما تسبّبه من ملأ منافذ الاتّصال، وكذا ملأ قوائم الانتظار.

3. 3- خداع بروتوكول الإنترنيت (IPSPOOFING): يتم ذلك بالتّخفي واستغلال بروتوكولات النّقل، بأن ينتحل المخترق صفة مستخدم آخر مخوّل بالاستخدام، ويقوم بتزوير العنوان المرفق مع خدمة البيانات المرسلة، ويظهر للنّظام وبروتوكولات النّقل على أنّه عنوان صحيح مرسل من داخل الشابكة[38] وبذلك يسمح النّظام لخدمة البيانات بالمرور باعتبارها خدمة مشروعة.

4- مخاطر القرصنة: من خلال استعراضنا لوسائل وأساليب القرصنة السّابق ذكرها يمكن تلخيص التّأثيرات الناتجة عن القرصنة وخطورتها على الأمن المعلوماتي للحكومة الإلكترونيّة في ما يلي:[39]

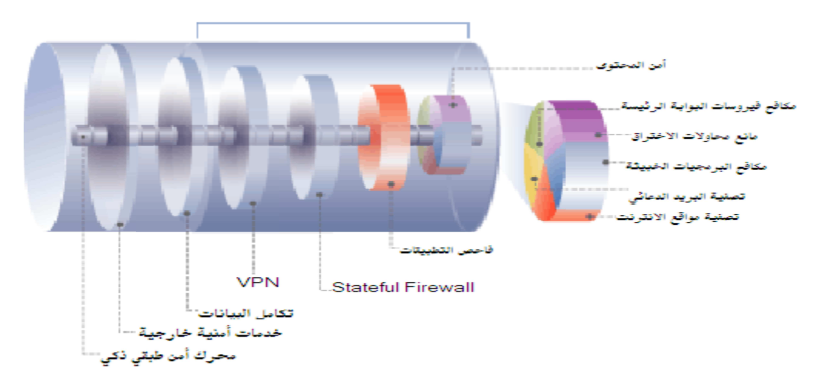
4. 1– **تدمير المواقع:** مثلما وسبق أن أشرنا لضخ الآلاف من الرّسائل الإلكترونيّة من جهاز الكمبيوتر الخاص بالمعتدي إلى المواقع.

4. 2– **تشويه المواقع:** يوجد تشابه كبير بين ما يحصل في العالم الافتراضي من عمليات تشويه مواقع ويب(D'effacement)، وبين ما يحدث على أرض الواقع عندما يتم إنزال علم دولة معيّنة من السفينة ورفع علم القراصنة مكانه. إنّ عملية التّشويه في أغلب الأحيان ليست سوى تغيير الصّفحة الرّئيسيّة للموقع بصفحة أخرى، فيها يعلن المخترق انتصاره على نظام مزوّد ويب والإجراءات الأمنيّة للشابكة، ويقصد من ورائها إبراز قدراته التّقنيّة، وإعلان تحدٍ للمشرفين على أنظمة مزوّدات ويب وتتضمّن الصّفحة الجديدة أحيانا رسالة يرغب الشّخص الّذي قام بعمليّة التّشويه بضللها للعالم، وقد تتضمّن اعتراضا منه على حالة سياسيّة أو اجتماعيّة، أو صرخة يريد إيصالها إلى كل من يزور هذا الموقع.

4. 3– **العبث بالبيانات:** بتغيير بيانات وإنشاء بيانات وهميّة في مراحل الإدخال، أو الإخراج، أو التّخزين.

4. 4– **الأخطار الماديّة للقرصنة:** يترتّب عن القرصنة خسائر ماديّة تتكبّدها الحكومات الإلكترونيّة.

توفر تقنيّة المعلومات وسائل متنوّعة لحماية الشابكات من أهمّها جدران الحماية (Firewalls)، والّتي عرفت قديما بالمصافي، وحديثا تطوّرت لتصبح تعرف بأجهزة حماية متعدّدة الخّصائص (UTM)؛ أي الإدارة الموحّدة للتّهديدات، وهذه الأخيرة لها خصائص متعدّدة في صندوق واحد، وتتضمّن تصفية البريد الإلكتروني الدّعائي (Spam)، وإمكانات الحماية من الفيروسات، وكشف، ومنع التّجسس (IDS /IPS)، وتصفية محتوى صفحات الويب، بالإضافة لمهام جدران الحماية التّقليديّة تصنّف جدران الحماية هذه على أنّها جدران لحماية طبقة التّطبيق (Aplication layer)؛ لذلك يمكننا العمل بالنّمط الشّفاف (Transparent mode) بحيث يتم إلغاء المستوى الأعلى من الفحص؛ ليكون جدار الحماية أكثر بساطة من بوابة تحويل عنوان الشابكة (NAT)، والشّكل يوضّح ذلك:[40]



يمثّل الشّكل أحد برامج الحماية والتّصدي من القرصنة المعلوماتيّة، ولاشك أنّ ثمة أهداف مسطّرة كونها تساهم في استراتيجية أمن المعلومات والمتمثّلة في:

– تعريف المستخدمين الإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية أنظمة الكمبيوتر والشابكات وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل إدخالها، ومعالجتها، وتخزينها، ونقلها، وإعادة استرجاعها؛

– تحديد الآليات الّتي يتم من خلالها تحقيق وتنفيذ الواجبات المحدّدة على كل من له علاقة بالمعلومات، والأنظمة وتحديد المسؤوليات عند حصول أي خطر؛

– بيان الإجراءات المتّبعة لتجاوز التّهديدات والمخاطر الّتي قد تصيب الأنظمة المعلوماتيّة وتنبيه الجهات المناط لها، والقيام بواجب الاحتياط منها.

خاتمة: يبقى الأمن المعلوماتي العربي ضرورة ملّحة يفرضها الواقع لقيام حكومات إلكترونيّة عربيّة محضة، ونحن نعترف أنّنا لم نصل بعد إلى المستوى الأمني المطلوب. إما للتّكلفة الباهظة الّتي تتطلبها أنظمة الحماية، وإما لقلة الخبرة والكفاءة في هذا المجال، ونحن نسعى دائما للتّقدم بخطوات واسعة في مجال المعلوماتيّة، ولاشك أنّنا بحاجة إلى حماية ما لدينا في مؤسّساتنا من مخاطر القرصنة أو الإرهاب المعلوماتي.

ولضمان استمراريّة العمل وجودة المعلومات المقدّمة تتزايد الحاجة يوما بعد يوم لمزيد من الوسائل والحلول لتعزيز حماية الأنظمة، كما لا يجب أن تنفك مراكز الأنظمة المعلوماتيّة في المؤسّسات المختلفة في البحث عن الآليات والوسائل الّتي تؤهّلها لحيازة أنظمة المعلومات الآمنة، وقلّما وجدت أنظمة آمنة بالكامل بل إنّ الحزم

بالنّظام الآمن بالكامل هو مستحيل لأنه من صنع وتنفيذ البشر؛ لتبقى الأنظمة الآمنة في الوقت الحالي ربّما لا تصلح لأن تكون آمنة بعد فترة وجيزة من الزّمن، وللاحتراز أو التّقليل من المخاطر والمهدّدات الأمنية يجب الأخذ بالنّتائج التّالية:

- تزويد مركبات الكمبيوتر بالتّقنيات المتطوّرة في مجال أنظمة الحماية؛
- استخدام برامج مكافحة الفيروسات لحماية جميع مكوّنات الأنظمة المعلوماتيّة؛
- استقطاب خبراء ومتميّزين في أمن أنظمة المعلومات للعمل بمراكز الحاسب الآلي؛
- توفير الحوافز الماديّة والمعنويّة المناسبة للمبدعين والمتفوقين في مجال حماية أنظمة المعلومات؛
- استخدام برامج الحماية الفعالة لمنع محاولات الاختراق والتّعدي على بيانات الكمبيوتر؛
- دعم ومساندة الإدارة العليا لسياسة تطبيق وسائل الحماية الماديّة والتّقنيّة؛
- الحرص على استخدام البرامج الأصليّة، وتجنب استخدام البرامج المنسوخة من الإنترنيت والعمل على تحديث برامج مكافحة الفيروسات باستمرار؛
- العمل على إنشاء إدارة من أصحاب الخبرة والدّراية بأمن أنظمة المعلومات؛ لتحديد التّقنيات اللاّزمة لحماية أجهزة الكمبيوتر.

الهوامش:

---

1 – ينظر: ندى اسماعيل جبوري "دراسة حالة في مصرف الرّافدين، فرع شارع فلسطين" مجلة تكريت للعلوم الإداريّة والاقتصادية، مجلد7، جامعة بغداد، كلّية الإدارة والاقتصاد: 2011م، ع21، ص77.

2 - M. Boudjemia. intelligence économique : concept définition et mode opératoire Séminaire de sensibilisation à l'intelligence économique et a la veille stratégique. Alger Algérie.23 décembre 2008.P:8.

3 – ينظر: عبد الفتاح بوخمخم وصالحي محمّد "الذّكاء الاقتصادي سياسة حوار بين المنظّمة ومحيطها" ضمن أعمال المؤتمر العلمي السّنوي الحادي عشر بعنوان: ذكاء الأعمال واقتصاد المعرفة، المنعقد ما بين: 23–26 أفريل 2012م، جامعة الزّيتونيّة الأردنيّة، كلّية الاقتصاد والعلوم الإداريّة، عمان– الأردن: 2012م، دع، ص352، 353.

4 – ينظر: الجمهوريّة اليمنيّة، مادة معلوماتيّة عن الأعمال الإلكترونيّة وأمن المعلومات، المركز الوطني للمعلومات: 2005م، عن الموقع الإلكتروني: wwww.arablaw.org، ص39.

5 – المرجع نفسه، ص 46، 48.
6 – ينظر: أيمن محد فارس الدّنف، واقع إدارة أمن نظم المعلومات في الكليات التّقنيّة بقطاع غزّة وسبل تطويرها، بحث ماجستير، الجامعة الإسلاميّة غزّة، عمادة الدّراسات العليا، كلّية التّجارة قسم إدارة الأعمال: 2013م، ص48.
7 – المرجع نفسه، ص32.
8 – ينظر: أسامة غربي، العولمة والجرائم المستحدثة، دط، معهد العلوم القانونيّة والإداريّة المركز الجامعي يحيى فارس، المديّة، دت، ص8.
9 – ينظر: أيمن محد فارس الدّنف، واقع إدارة أمن نظم المعلومات في الكليات التّقنيّة بقطاع غزّة وسبل تطويرها، ص61.
10 – المرجع نفسه، ص61.
11 – ينظر: عبد الفتاح بوخمخم وصالحي محمّد، الذّكاء الاقتصادي سياسة حوار بين المنظّمة ومحيطها، ص 354.
12 – ع/أيمن محد فارس الدّنف، واقع إدارة أمن نظم المعلومات في الكليات التّقنيّة بقطاع غزّة وسبل تطويرها، ص 62.
13 – المرجع نفسه، ص 62.
14 – الحماني علاء حسين وألعاني سعد عبد العزيز، تكنولوجيا أمنيّة المعلومات وأنظمة الحماية ط1، عمان: 2007م، دار وائل للنّشر والتّوزيع، ص 22.
15 – ينظر: بسيوني عبد الحميد، حماية الحاسبات والشّبكات من فيروسات الكمبيوتر والملوثات ط1، القاهرة: 2007م، دار الكتب العلميّة للنّشر والتّوزيع، ص 193، 194.
16 – المرجع نفسه، ص 194.
17 – ينظر: ميراي رعد، "هل تعرف كل شيء عن الإنترنيت حقا؟" مجلة الأمن الرّقمي في العالم العربي، دب: 2011م، ع1، عن الموقع الإلكتروني: http: // www.cyber –arabs.com، ص28.
18 – المرجع نفسه، ص 29.
19 – ينظر: الحميد محمّد دباس ونينو ماركوا إبراهيم، حماية أنظمة المعلومات، دط، عمان: 2007م، دار الحامد للنّشر والتّوزيع، ص 166.
20 – المرجع نفسه، ص 166.
21 – ينظر: عائشة إبراهيم البريمي، تقنية البلوتوث (الإيجابيات، المخاطر، الحلول) –دراسة ميدانيّة– مركز بحوث شرطة الشارقة، عن الموقع الإلكتروني: http : // www.alriyadh. Com ص،8–11.
22 – ينظر: عبد العزيز بن حمد الزّومان، شبكة الإنترنيت دليل تعريفي، دط، المملكة العربيّة السّعوديّة: 1422هـ، مدينة الملك عبد العزيز للعلوم التّقنيّة، وحدة خدمات الإنترنيت، ص27.

23 – ينظر: جمهوريّة العراق، هيئة الإعلام والاتصالات، مبادئ توجيهيّة لحماية أبنائنا من خطر الإنترنيت، عن الموقع الإلكتروني: WWW.CMC.TQ. ص 12.

24 – المرجع نفسه، ص 12.

25 – ينظر: عبد الفتاح بوخمخم وصالحي محمّد، الذّكاء الاقتصادي سياسة حوار بين المنظّمة ومحيطها، ص 355.

26 – ينظر: زكريا أحمد عمار، حماية الشّبكات الرّئيسيّة من الاختراق والبرامج الضّارة، بحث ماجستير، جامعة النيلين، كليّة الدّراسات العليا: 2011م، ص 67.

27 – ينظر: سوزان فيشر، مجلة الأمن الرّقمي في العالم العربي، دب: 2013م، ع0، عن الموقع الإلكتروني: http:// www.cyber-arabs.com، ص 25.

28 – ينظر: عبد الفتاح بوخمخم وصالحي محمّد، الذّكاء الاقتصادي سياسة حوار بين المنظّمة ومحيطها، ص 356.

29 – ينظر: ميراي رعد، هل تعرف كل شيء عن الأنترنيت حقا؟ ص9.

30 – ينظر: الجمهوريّة اليمنيّة، مادة معلوماتيّة عن الأعمال الإلكترونيّة وأمن المعلومات، المركز الوطني للمعلومات: 2005م، عن المقع الإلكتروني: wwww.arablaw.org، ص 41.

31 – المرجع نفسه، ص 42.

32 – ينظر: ليتيم فتيحة وليتيم ناديّة، "الأمن المعلوماتي للحكومة الإلكترونيّة وإرهاب القرصنة" مجلّة الفكر، الجزائر: دت، كلّية الحقوق والعلوم السّياسيّة، ع12، ص242.

33 – منير محمّد الجنبيهي وممدوح محمّد الجنبيهي، أمن المعلومات الإلكترونيّة، دط الإسكندريّة: 2006م، ص13.

34 – المرجع نفسه، ص 13.

35 – ليتيم فتيحة وليتيم ناديّة، الأمن المعلوماتي للحكومة الإلكترونيّة وإرهاب القرصنة، ص243.

36 – المرجع نفسه، ص 244.

37 – ينظر: ناديّة أمين محمّد علي، الفيروسات وطرق الوقاية منها كأمن البيانات، ضمن أعمال المؤتمر الدّولي لأمن المعلومات الإلكترونيّة: نحو نحو تعامل رقمي آمن، عمان: 2005م، ص205.

38 – ينظر: صفيّة أحمد أبو بكر، استخدام (IPSEC) كوسيلة لحماية الشابكات من الهجمات الفّعالة، ضمن أعمال المؤتمر الدّولي حول: أمن المعلومات نحو تعامل رقمي آمن، مسقط: 2005م، ص 218.

39 – المرجع نفسه، ص 218.

40 – زكريا أحمد عمار، حماية الشّبكات الرّئيسيّة من الاختراق والبرامج الضّارة، ص 57.

جهود المنظّمة العالميّة للتّقييس الأيزو ISO في تحقيق الأمن المعلوماتيّ

أ. أحلام بن عمرة

جامعة مولود معمري، تيزي-وزو

مقدمة: إنّ موضوع الأمن المعلوماتي موضوع في غاية الأهمّية، ويمسّ بشكل مباشر حياة كلّ المتعاملين مع الوسائط الإلكترونيّة، وينعكس على مصالحهم وسبل أداء أعمالهم، ويرتبط ارتباطا وثيقا بأمن الحاسوب، فلا يوجد أمن للمعلومات إن لم يراعى أمن الحاسوب، وفي ظل التّطورات المتسارعة في العالم، والتّي أثرت على الإمكانات التّقنيّة المتقدمة المتاحة، والرّامية إلى خرق منظومات الحاسوب؛ بهدف السّرقة أو تخريب المعلومات، أو تدمير أجهزة الحاسوب، كان لا بد مكن التّفكير الجدي؛ لتحديد الإجراءات الدفاعيّة والوقائيّة، وحسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب.

مما لا شك فيه أنّ المعلومات تلعب دورا مهمّا في حماية أصول الشّركة أو المؤسّسة، وكثيرا ما نسمع في الأخبار عن الحوادث الأمنية للأمن المعلوماتي، مثل تشويه المواقع، وتسرب المعلومات؛ ولذلك المنظمات بحاجة إلى أن تدرك الحاجة إلى تكريس المزيد من الموارد؛ لحماية أصول المعلومات، وأمن المعلومات يجبب أن يصبح مصدر قلق كبير في كل من الحكومة وقطاع الأعمال.

ولما كان من المستحيل حماية المؤسّسة أو الشّركة بنسبة 100 % بات من الضروري وضع مجموعة من المقاييس، أو المعايير التّي يمكن من خلالها تحقيق مستوى ملائم من الأمن.

ومن خلال هذه المقدّمة فإننا سنذكر أهم المعايير العالمّية التّي تساعد على تحقيق الحد الأدنى المعلومات مثل: الأيزو 27001ISO هو أحد سلسلة عائلة المعايير 27000ISO الصادرة عن المنظمة العالمية للمعايير، وهو يصّف الاحتياجات إلى إنشاء وتشغيل ومراقبة ومراجعة وصيانة، وتحسين نظام إدارة أمن معلومات موثق باستخدامه منهاج التّحسين المستمر، هذا المعيار لا يفرض كما يظن البعض ضوابط أمنية معينة، أو يعالج فقط النواحي الأمنيّة لتقنية المعلومات بل إنّه يقف فقط على مستوى إدارته لنظام الأمن المعلوماتي، أما من يقوم بدور إرشادي لتّفسير، وتطبيق الضوابط في ملحقه فهو معيار قواعد الممارسة لإدارة أمن المعلوم ISO 27002 المنتمي على نفس العائلة؛ وعليه يجيب مقالي على إشكالية في غاية الأهميّة وهي كيف تحمي منظمة العالميّة للتّقييس الأيزو المعلومات؟ وماهي خطوات تطبيق مواصفة الأيزو ؟ وماهي فوائدها؟

1 - مفهوم المنظمة العالمية للتّقييس الأيزوISO

1-1- المنظمة: ORGANISATION هيأة مكوّنة، لها أهداف محدّدة "وقانون يرسم أعمالها ومبادئها تعمل على تحقيقها في مجال اهتمامها في السّياسة أو النّقابة أو الثّقافة"[1].

2-1 - العالميّة: INTERNATIONNALE اسم مؤنث منسوب إلى عالم "وهي حركة إنسانيّة تعمل على خدمة البشريّة والتّقارب بين الشّعوب دون المسّاس بهويتها وخصوصيتها الثّقافية[2]".

1-3- مفهوم التّقييس: NORMALISATION كلمة تقييس هي الّتي تتداول في اللّغة العربية لمقابلة المصطلح الفرنسي Normalisation والمصطلح الإنجليزي Standardization ويعرف التّقييس على أنّه" **صيّاغة وتطبيق مجموعة من القواعد والشّروط التّي تستهدف تنظيم وتوجيه نشاط ما يهدف إليه تحقيق الفائدة المرجوة من الأطراف ذوي العلاقة وتعزيز تعاونها من أجل تأمين الاقتصاد المطلوب في فعاليته**"[3] فالتّقييس نشاط خاص يرمي إلى إعطاء حلول لتطبيقات متكرّرة في مختلف الحقول، والميادين العلميّة، التّكنولوجيّا، الاقتصاديّة وذلك من أجل البلوغ بها في سياق معيّن إلى مستوى أمني من النّظام يتّجسد فيه النّشاط في صيّاغة مواصفات ونشرها، وتطبيقها.

1–4 – مفهوم مصطلح الإيزوISO: تعني الإيزو من حيث معنى الكلمة بأنّها "تعني التّبادل أو التّساوي والتّشابه"[4] وهي كلمة مشتقة من أصل يوناني إيزوس ISOS مستنبطة من "فكرة عدم الاختلاف أو التّعادل"[5]؛ ولهذا فإنّ المقصود بكلمة إيزو هو وجود مواصفات قياسيّة متجانسة لعمليّة معيّنة قادرة على إنتاج وحدات متماثلة،. ويتمثّل الدور الرئيسي لهذه المنظمة في إصدار مواصفات دوليّة موحدة سواء كانت فنيّة تخص السّلع، أو الخدمات تتعلّق بالنّظام التّعليميّ أو الاقتصاديّ...الخ، هذا بالإضافة إلى أنّها تعمل على رفع المستويات القياسيّة ووضع المعايير والأسس والاختبارات، ومنح الشهادات المتعلّقة بها من أجل تشجيع خدماتها على مستوى عالميّ في أغلب المجالات، بناء على ما سبق يمكن تعريف المنظمة الدوليّة للمواصفات القياسيّة الآيزو على أنها «منظمة مهتمة بإصدار المواصفات القياسيّة الدوليّة وتوحيد المواصفات في المجالات المتعدّدة على المستوى العالميّ حتّى تساعد على سهولة التبادل التّجاري في السّلع والخدمات، وتطوير التّعاون بين دول العالم»[6]، وهذا ما يعطي للمنظمة سمّة العمل

و يضمن لها تحقيق الجودة في مختلف منتجاتها، من خلال حرصها على التّقييم المستمر.

2- مفهوم معيار الإيزو 27001: عبارة عن معيار متكامل لبناء أمن معلومات فعّال قابل للتّطوّر المستمر، ويخضع للتّقييم من جهة محوّلة بذلك مرّتين خلال السّنة، ويعطي الحصول عليه مزيد من الثّقة بالجهة الحاصلة على الشّهادة من ناحيّة حمايتها لمعلوماتها ومعلومات عملائها[7].

إنّه عبارة عن تطوير، تنفيذ، تشغيل، مراقبة، مراجعة محافظة على، وتحسين نظام أمن معلومات موثق في المنظمة يهدف إلى إدارة فعّالة، ومستمرة للمخاطر تقوم بحماية مناسبة للمعلومات حسب أهمّيتها. كما نشير إلى أنّ كلمة نظام الواردة هنّا لا تعني نظام إلكتروني أو معلوماتي، بل نظام يعتمد على عمليّات مستمرة يؤدي تطبيقها إلى الحماية المرجوة، والتّطور المستمرة بناء على منهجيّة معتمدة.

3 - مفهوم الأمن المعلوماتي: الأمن المعلوماتي، من زاوية أكاديميّة، هو العلم الّذي يبحث في نظريّات، واستراتيجيّات توفير الحماية للمعلومات من المخاطر التّي تهددها. ومن زاوية تقنيّة، هو الوسائل، والاجراءات اللاّزم توفيرها؛ لضمان حمايّة المعلومات من الأخطار الداخليّة والخارجيّة، ومن زاوية قانونيّة؛ فإنّ الأمن المعلوماتي هو محل دراسّات، وتدابير حمايّة سريّة، وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها، وهو هدف وغرض تشريعات حمايّة المعلومات من الأنشطة غير المشروعة، وغير القانونيّة التّي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت)، وقد عرّف على أنّه "بأنّه مجموعة من الإجراءات والتّدابير الوقائيّة الّتي تستخدم سواء في المجال التّقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيّات إضافة إلى الإجراءات المتعلّقة بالحفاظ على العاملين في هذا المجال؛ الحفاظ على المعلومات المتواجدة في أي

نظام معلوماتي من مخاطر الضيّاع أو التلف"[8]. واستخدام اصطلاح الأمن المعلوماتي Information Security وإن كان استخداما قديما سابقا لولادة وسائل تكنولوجيّا المعلومات، إلا أنّه وجد استخدامه الشّائع، بل والفعلي في نطاق أنشطة معالجة ونقل البيّانات بواسطة وسائل الحوسبة والاتصال، إذ مع شيوع الوسائل التّقنيّة لمعالجة، وخزن البيانات وتداولها والتّفاعل معها عبر شبكات المعلومات– وتحديدا الإنترنت – احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النّماء من بين أبحاث تقنيّة المعلومات المختلفة، بل ربّما أمست أحد الهواجس التّي تؤرق مختلف الجهات .

4- عناصر الأمن المعلوماتي: تنقسم عناصر الأمن المعلوماتي إلى ثلاث عناصر منها:

4-1.- سريّة المعلومات: تعني "ضمان المعلومات المخزنة، أو المنقولة عبر الشّبكة وعدم الاطلاع عليها أو استخدامها إلا بموجب إذن"[9]. وتهدف سريّة المعلومات إلى التّأكد من عدم إطلاع غير المصرح لهم عليها، فضلا عن تحديد حدود، وصلاحيّة الاستخدام سواء كان كليّ أو جزئيّ، مع تحديد من له صلاحيّة التّعديل أو الإدخال أو الحذف أو الإضافة أو القراءة فقط من بين المصرّح لهم بوجه عام.

4-2 - سلامة المعلومة: تعني ضمان عدم تغييّر المعلومات المخزنة أو المنقولة؛ حيث يتكون عنصر سلامة المعلومة من شقين: "الأول سلامة المعلومة والثّاني سلامة المصدر؛ فالمفهوم الصحيح لسلامة المعلومة هو عدم تغييرها بشكل غير ملائم سواء بقصد أو بغير قصد، وأنّها أدخلت بشكل صحيح يعكس الظروف الحقيقيّة للمعلومة[10]. أما سلامة المصدر؛ فيقصد بها الحصول على المعلومة من مصدرها الأصّلي. وتشير سلامة المعلومات بصفة عامّة إلى الإجراءات التّي

تضمن حفظ المعلومات خلال مراحل إدخالها، أو نقلها بين الأجهزة، والشّبكات للمحافظة على سريتها وسلامتها.

4 -3 - توافر المعلومات: يعني "ضمان بقاء المعلومات وعدم حذفها أو تدميرها"[11]. وأهم الأخطار التّي تهدّد توافر المعلومات هي:

– رفض (منع) الخدمة: يعني الأعمال التّي تعطل نظم الحاسب وشبكاته بصورة لا تمكن المصرّح من استخدام الحواسيب والاستفادة منها. والوصول إلى المعلومات؛

– فقدان القدّرة على معالجة البيّانات نتيجة الكوارث الطبيعيّة، وأو الأفعال العمديّة.

5 -. الفرق بين الإيزو 27001 والأيزو 27002.

1 - الإيزو 27001: عبارة عن معيار عالميّ يعني بحماية المعلومة له متطلّبات معيّنة عند تلبيّتها تحصل المنظمة على شهادة معتمدة يتقيّد تطبيقها بالمعايير الواردة على نطاق العمل الّذي تمّ اختياره بمعنى أنّه:

– يتّم تقييم مدى التوافق مع المعايير ويحصل دورين مرتين خلال العام؛

– بعد اجتيـــازه للتقييـــم تحصل المنظمة على شهادة معتمدة بموافقتها للمعيار 27001.

2– الأيزو 27002: عبارة عن أفضل الممارسات والتّوجيهات في تطبيق ما ورد في المعيار 27001 من أدوات تحكّم تعني المعلومات كما أنّه لا يقدّم توجيهات حول طريقة تنفيذ المعيار 27001 وإنّما توجيهات حول كيفيّة تطبيق أدوات التّحكم كما ورد في التّعريف،. ولا يستخدم في التّقييم بمعنى أنّه لا يتّم تقييم مدى تطبيق المنشأة لمعيار 27002 من جهة خارجيّة.

6- عمليّات تطبيق المواصفة ISO 27001 وفوائد تطبيقها: تعدّ المواصفة الأيزو 27001 مواصفة معياريّة؛ لأي مؤسّسة، والتّي ترغب في الحصول على شهادة مستقلة لنظام إدارة حمايّة المعلومات الخاصّة بها، وينقسم نظام أمن المعلومات إلى أربع مراحل مستمرة وهي: التّخطيط ؛ أي وضع خطة (Plan) التّنفيذ (Do): البدء في تنفيذ الخطط وتشغيلها: التّحقق (Check): مراجعة النّظام بعد تنفيذه، وأخيرا العمل (Act) ونقوم بالتّدريج بتطبيق هذه الخطوات بالتّفصيل:

6-1- تكوين لجنة أمن المعلومات: وتعنى هذه اللّجنة بتطوير السّياسة العامة لأمن المعلومات واعتمادها؛

- تطوير أهداف أمن السّياسة العامة لأمن المعلومات واعتماها؛
- تطوير أهداف الأمن والتّأكد من توافقها مع أهداف المنشأة؛
- إدارة المصادر الخاصّة لإدارة أمن المعلومات؛
- مراجعة نتائج تقارير تقييم المخاطر ومدى تأثيرها على العمل؛
- تطوير خطط معالجة المخاطر؛
- إدارة تنفيذ خطط معالجة المخاطر؛
- التّأكد من تطوير نظام إدارة أمن المعلومات في المنظمة؛
- التّأكد من أن التّعامل مع الأحداث الأمنيّة مثل الوقوع تحت هجمات إلكترونيّة، انتشار الفيروسات يتّم بشكل جيد.

6 –2 – أعضاء اللّجنة: تحتاج اللّجنة أن تدّعم من الإدارة العليّا بشكل محكّم؛ وذلك لتفعيل نظام الأمن المعلوماتي، كما ينصح أن يترأسها المدير التّنفيذي، أو من ينوبه، أو من يكون في مركز مساوي في القطاعات غير التّجارية، كما يجب أن تحتوي اللّجنة على أعضاء أصحاب قرار في المنشأة، ولهم علاقة مباشرة بإدارة المعلومات والأعمال، ومن ذلك عضو من التّشغيل، عضو من الشّؤون الإداريّة

والماليّة عضو عن إدارة شؤون الموظفين، عضو من إدارة الجودة من عضو من تقنيّة المعلومات، عضو من إدارة المبنى، ونحوه ويعتمد ذلك على كل من المنظمة والهيكل التّنظيمي لها.

كما نشير إلى ضرورة تعييّن مدير لنظام الأمن المعلوماتي، ويكون أحد أعضاء هذه اللّجنة، ثمّ اختيار نطاق العمل والأهداف؛ حيث يتمّ في هذه المرحلة تحديد النّطاق الّذي يتمّ حصول الشّهادة عليه على أن يكون اختيار النّطاق بناء على أهداف، وأعمال المنظمة، فمثلا لا ترغب إدارة تقنيّة المعلومات بالحصول على شهادة الأيزو 27001 على مركز البيّانات، والّذي يحتوي على الخوادم، ونحوها والّتي بدورها على جميع معلومات المنظمة، ومن كان في حمايّة المعلومات في النّطاق يدعم حماية عمل المنظمة، ومن هنا يتميّز هذا المعيار بأنّه يكفي لتحديد النّطاق، وأن يكون حمايّة مصادر المعلومات في نطاق العمل بعيد عن نطاق عمل المنظمة، وقد يساعد تحديد أهداف المنظمة، خدماتها ومعرفة الهيكل التّنظيمي في اختيار النّطاق، كما يجب الأخذ بالاعتبار الأنظمة المستخدمة، والجهات ذات العلاقة.

كما ننوه أن نطاق العمل لا يستلزم أن يكون العمل في بيئة إلكترونيّة، بل الأهم من ذلك وجود معلومة يوفر حمايتها حمايّة لمصادر المنظمة ويدّعم تحقيق أهداف المنظمة.

3-6 - كتابة السّياسة: بعد تحديد النّطاق يلزم كتابة السّياسة العامّة للأمن المعلوماتي في النّطاق، والتّي تتضمن خطوط عريضة تضمن الالتزام بحمايّة المعلومات، وتوضح التزام الإدارة العليا بالأمن المعلوماتي، وقد يتمّ اعتمادها من أعلى جهة في المنظمة بناء على اعتمادها من لجنة المعلومات.

4-6- تطوير منهج تقييم المخاطر: والّذي سيتم اتباعه خلال تحليل، وتقيّيم المخاطر لمصادر المعلومات في نطاق العمل، ويحتوي ذلك على خطوات توضح عمليّة تحديد، وتحليل المخاطر؛ بحيث يتمّ معرفة أصول المعلومات إلكترونيّة ورقية، أدوات، أجهزة قيمة هذه الأصول، ومن ثمّ معرفة ما هي التّهديدات والثّغرات المحتملة، ومدى تأثيرها على المعلومة وتغيّيرها ونحوها. كما نشير إلى أنّه عند كتابة منهج تقييم المخاطر ينصح بأن يأخذ بعين الاعتبار أنّ حماية المعلومة لا يجب أن يتعدّى قيمتها. ومن هنّا يتم العمل على الحماية اللازمة لأصول المعلومات، وذلك باختيار طرق الحماة التّي تتناسب مع بيئة المنظمة؛ وذلك باختيار طرق الحمايّة من قائمة يوفّرها المعيار كملحق له، ولا يلزم جميع الطّرق ما يلزم لحماية المعلومة واحتواء الخطر، ويكون ناتج هذه المرحلة تقرير تقيّيم وتحليل المخاطر، وتقليلها بعد اختيار طرق الحمايّة اللازمة ويتضمن حساب المخاطر تطبيق طرق الحمايّة.

5-6- التّوعية الأمنيّة: يتّم بعد ذلك عمل برنامج توعيّة أمنيّة للموظفين داخل نطاق العمل والّذي تمّ تحديده في الخطوة الأولى، وقد يشمل البرنامج على عروض تقييميّة توعويّة، ودورات تدريبيّة أو تعليم ويحتوي البرنامج أيضا على ترويض البيّانات، وإجراءات من المعلومات، والتّي تم تطويرها كجزء من المرحلة السّابقة وتعريف الموظفين في إطار العمل على أي إجراءات جديدة والتّأكد من توافق أعمالهم مع ما تمّ في الإجراءات المراقبة والتّطوير المستمر لنظام أمن المعلومات وتحتوي على:

- مراجعة الأحداث الأمنيّة، والعمل على معرفة السّبب الرئيسي والتّعامل معه؛
- مراجعة سياسّة أمن المعلومات بشكل دوري، هو الهدف من النظام؛
- مراجعة تقارير تحليل وتقييم المخاطر، ومستوى الخطر المقبول؛

– مراجعة ما تمّ تطبيقه من طرق الحمايّة الّتي تمّ اختيارها ملحق معيار A annexe.

6-6- مراجعة تقارير التّدقيق الداخلي والخارجي: رفع تقارير نتائج المراجعات للجنّة الأمن المعلوماتي، والمسؤول عن نظام أمن المعلومات واستخدامها؛ لتطوير النّظام بشكل عام؛ بحيث قد يشمل التّطوير على تطوير الهيكل التّنظيمي، تطوير التّقنيّة، مراقبة التّهديدات المستقبليّة، وبناء الخطط الملائمة للتّعامل معها، وفهم الأنظمة، والقوانين الجديدة المتعلقة بنطاق العمل، أو بالمنظمة ككّل، والّتي بدورها ستؤثر على نظام العمل الأمن المعلوماتي.

7-6- المحافظة على نظام الأمن المعلوماتي: ويتمّ تطبيقهما ما توصّل إليه في الخطوة السّابقة واتّخاذ ما يلزم لتصحيح بعض الأخطاء، والتّي تمّ استخلاصها من الأحداث الأمنيّة، والتّقييم الدّاخلي والخارجي ومحاولة منع حدوثها في المستقبل. كما نشير إلى ضرورة تبادل المعلومات في ما يخص المحافظة على الأمن المعلوماتي.

8-6- التّدقيق الدّاخلي: ويفضل أن يقوم بهذه المرحلة فريق مستقل عن الفريق الّذي قام بتطوير نظام أمن المعلومات من خلال نموذج العمل (PDCA) Plan- Do-Check، الّذي يقوم بعمل التّحسين المستمر وبهذا تستند المواصفة ISO 27002 في عملها على تسعة أجزاء للمعالجة، يمكن تلخيصها بالآتّي:

– تعريف المجال لنظام وإدارة وسياسة حماية المعلومات ISMS، وتقيّيم وإدارة الأخطار والمخاطر والتّحليل؛

– تحديد الأهداف للسّيطرة، والسّيطرة الفعليّة عليها/ التّطبيق. وتجهيز بيان (قائمة أو كشف) التّطبيق؛

– تطبيق وتشغيل واستمرار المراقبة وإدامة وتحسين ISMS.

8- هيكلة المواصفة وخطوط عملها العريضة: تستعرض المواصفة عدد من الإجراءات والعمليّات ينقسم التّي يجب على المؤسّسة تنفيذها عند التّعامل مع البيانات، والمعلومات الورقيّة والرقميّة بحيث تغطي المحاور التّالية:

8- 1- سياسة أمن المعلومات: مجموعة من القوانين والمعايير التّي تتمّ كتابتها واعتمادها ومن ثمّ تطبيقها لحمايّة المعلومات في نطاق العمل الّذي تمّ اختياره ومثال ذلك: "تعتبر معلومات المؤسّسة أحد أصول المؤسّسة، وتعدّ حمايتها أمر أساسيّ لاستمراريّة العمل. وتعدّ المحافظة على صحة وسريّة وسلامة المعلومات أمورا حتميّة؛ لتحقيق أهداف المؤسّسة التّنظيميّة والقانونيّة والتّعاقديّة. وبناء عليه سيتّم اتخاذ جميع ما يوفر الحمايّة اللاّزمة؛ لهذه الأصول سواء من حيث الاستخدام الغير المصرح به أو التّعديل أو الكشف عنها سواء أكانت المحاولات عرضيّة أو معتمدة، ويلتزم جميع الموظفين والمتعاقدين والأطراف العاملة، داخل المؤسّسة بحماية المعلومات وتنفيذ سيّاسة وإجراءات أمن المعلومات"[12] وهذا إن دلّ على شيء إنّما يدّل على أنّ أصول المعلومات لا تقل أهميّة عن المعلومات وأنّ حمايتها واجب وخطوة تعمل لصالح حماية المعلومات.

8-2- تنظيم أمن المعلومات: Organization of information security

ويسعى إلى التّأكد من إدارة أمن المعلومات في المؤسسة، "وتوضيح المهام والمسؤوليّات ذات العلاقة سواء داخل المؤسسة من إدارات داخليّة، أو خارجها من جهات تتعامل معها، ويعتبر وجود تنظيم واضح لأمن المعلومات في المؤسسة مؤشرا هام للالتزام بحماية المعلومات"[13] وهو أحد متطلّبات المواصفة العالميّة كما يعد وجود لجنة أمن المعلومات أحد مؤشرات تنظيم الأمن المعلوماتي، وتتولى هذه اللّجنة التّي يجب أن يكون من أعضائها خبراء في مواجهة الاختراقات الأمنية وضع سياسات واضحة، أما الإدارة العليا والمتوسطة فيجب أن يكون لديها أهداف

واضحة عن سياسة أمن البينات داخل المركز، وأن تظهر التزام واضح تجاه سرية وأمن البيّانات.

8–3– إدارة الأصول: Asset management يعرف "الأصل على أنّه أيّ شيء له قيمة للمؤسّسة"[14]، وتهدف إدارة الأصول إلى توفير حمايّة تتناسب وأهميّة الأصول؛ بحيث يتم أولا معرفة وتحديد جميع الأصول الماديّة: عن أجهزة وخوادم ومعدات الشّبكة والاتّصالات وقواعد بيّانات وموارد بشرية، وغيرها، أو غير ماديّة مثل: سمعة المؤسّسة، ومعرفة مدى قيمة هذه الأصول. ويتّم بعد ذلك بالتّخطيط لحمايتها، وتوفير الحلول المناسبة. على أن يتّم جرد أو حصر كافة الأصول الخاصّة بمراكز المعلومات، وتسجيلها في سجلات الأصول، وإجراء كافة العمليّات الفنيّة والماليّة والاحتفاظ بها بدّقة.

8– 4– أمن الموارد البشرية (الموظفين، المتعاقدين، ونحوهم) Human resources security ونعني به تحديد المسؤوليّات والمهام للموظفين والمتّعاقدين ونحوهم، والاعتناء باختيارهم بما يتوافق مع المعلومات التّي سيتعامل معها كل فرد بناء على سياسات أمن المعلومات، ومثال ذلك أنّه عند الحاجة لتوظيف مدير قواعد بيانات على سبيل المثال، وبناء على أنّ قواعد البيّانات للمؤسّسة تحتوي على جميع المعلومات الحسّاسة، يجب أن يتّم أولا الاختبار بعنايّة، ويتّم بعد ذلك عمل التحقق من خلو سجله العمليّ من أي سوابق غير متلائمة مع الوظيفة التّي سيعمل عليها وعند التّوظيف يتّم تعريفه بالمهام والمسؤوليّات وتوقيعه كأي موظف على وثيقة عدم إفشاء المعلومات والمحافظة عليها.

وبمعنى أنّ هذه المواصفة تعني بعمليّة إدارة الموظفين كعمليّة متكاملة ابتداء من اختيار الموظف، قبل التّوظيف، وخلال التّوظيف، وخلال ممارسة الوظيفة ومن ثم عند انتهاء الخدمة أن يتمّ أوّلا التّأكد من إنهاء جميع الإجراءات، بالشكل المناسب

مثل التّأكد من إيقاف جميع حسابات الذي أنهى خدماته مباشرة واسترجاع جميع ما لديه من أصول.

8– 5– الأمن البيئي والمادي: Physical and environmental security

وهو حماية موارد، و أصول المؤسّسة من الوصول إليها والعبث بها؛ وذلك بتوفير أدوات حماية مناسبة للمباني ومراكز البيّانات التّي تحتوي على الأجهزة، والخوادم والمكاتب والأجهزة، والملحقات. كما يجب أن نأخذ بعين الاعتبار هنا المخاطر الطبيعيّة مثل الأمطار والفيضانات، ومن أدوات الحمايّة توفير سياسات وإجراءات للدخول إلى مراكز البيّانات، ونقل وتحميل الأجهزة من مكان إلى آخر سواء داخل المبنى أو خارجه، وهذا يتطلّب تجهيز المباني التّي تحتوي على بيانات رقميّة بالمعدّات والأجهزة، ووضع نظام محكم لحفظ بيّانات الدخول والخروج والاحتفاظ بها لفترة زمنية بصورة آمنة، ومن دون أن تتعرض للإلغاء أو المسح بقصد أو بدون قصد.

8 – 6 – إدارة الاتّصالات والتّشغيل: وتهتم بإدارة الاتّصالات، وعمليّات التّسجيل الخاصّة بتقنية المعلومات، وأن يراعى هنّا المحافظة على سريّة المعلومات، وتوفرها عند الحاجة والمحافظة على سلامة محتواها من التّغيير الغير مصرح به[15]؛ بحيث يتمّ تطوير إجراءات تشغيله للتّعامل مع تقنية المعلومات وخصوصا ما يتعلق بنطاق العمل الذي تمّ تحديده، والعناية بتوزيع المهام بشكل مناسب بما يوفر الحماية المطلوبة، ويمنع التّغيير الغير مصرح به أو العبث بأصول المؤسّسة، وذلك أن يتم الفصل بين بيئة التّطوير للبرامج وبيئة اختبارها والبيئة التّشغيلية، ومثل فصل مهام تشغيل الشّبكة عن مهام مراقبة أمن المعلومات.، كما يجب الاعتناء هنا بتوفير حماية المعلومات، والتّي يتمّ الوصول إليها من جهات خارجيّة وذلك بتوقيع اتفاقيات توضيح المهام والمسؤوليات

ومستوى الخدمة المطلوبة، والعواقب المترتبة على الإخلال بذلك والطريقة الملائمة لتناقلها، وأيضا يتّم هنا مراقبة وتحسين مستوى الاستفادة لمصادر المعلومات ودراسة وتخطيط الزيادة المتوقعة، وتطوير إجراءات مراقبة البرامج الضارة، مثل الفيروسات ومنع استخدامها، واستخدام الحلول التي تساعد في ذلك، وتطوير إجراءات أخذ النّسخ الاحتياطيّة واختبارها، وتخزينها في مكان ملائم، مثل تخزينها في موقع آخر ليتم استيرادها عند الحاجة، أو استرجاع البيّانات في حالة حوادث طارئة طبيعيّة أو بشريّة، وإدارة الشّركة بطريق آمنة؛ وذلك ببناء هيكلة آمنة للشّبكة تحمي المعلومات المتناقلة بها، والتّطبيقات البرمجيّة، والأنظمة المترابطة عن طريقها، والتّي تسمح بإدارتها بشكل آمن، مع استخدام أنظمة للدخول إلى الشّبكة ومراقبتها بشكل مستمر، والحفاظ على سجلات الدخول والخروج والاستعمال للرجوع إليها عند الحاجة.

8-7- التّطوير والصيانة لأنظمة المعلومات: تعني هذه المواصفة بأهميّة توضح متطلّبات الأنظمة البرمجيّة التّي يتم توريدها من النّواحي الأمنيّة، والتّأكد من معالجة المعلومات بطريقة تتناسب وأهميّتها وسريتها وتحافظ على ملفات النّظام تمر البيانات بعدد من المراحل، وبالتّالي فإنّ البرمجيات التّي تقوم بمعالجتها هي الأخرى تمرّ بذات مراحل التّطوير التّحديث والاستبدال، وتؤكد هذه المواصفة على المحافظة على سريّة وأمن البيانات المتعلّقة بالبرمجيّات الداخليّة في النّظام، فعند إضافة برمجيات أو تطبيقات برمجيّة جديد على مراكز المعلومات، وإدارة الأحداث الأمنيّة: يتّم هنا تعريف السياسات والإجراءات الخاصّة بالتّعامل مع الأحداث الأمنيّة، وطرق احتواءها ومنع أو التّقليل من تأثيرها على البيّانات والمعلومات داخل النّظام، وسير العمل ودراسة مسبباتها لتجنبها في المستقبل. ويجب وضع آليّة واضحة في مراكز المعلومات للتّبليغ عن أيّة اختراقات أمنيّة أو حوادث عمل على

أن توضح هذه الآليّة طرق الاتّصال بالإدارة للتّبليغ من الحادثة، وتوثيق جميع الخطوات التّي يجب إنجازها في معالجتها.

8–8– إدارة استمرارية الأعمال: Business continuity management يتّم هنا تطوير الخطط الكفيلة بضمان استمراريّة العمل حتى حال حصول بعض المشاكل التّقنية، مثل: عطل في أحد الخوادم، وانقطاع الكهرباء، وتعطل أحد المواجهات أو حتى تغيب أحد الموظفين واختيارها دوريا وتحسينها بما يتلاءم ومتطلبات المؤسسة، وهذه المشاكل الفنية التي تواجهها تعود إلى المواصفات المبدئيّة التّي تمّ الاعتماد عليها عند إعداد المشروع، هذا مع العلم بأنّ لكل مكون من مكوّنات النّظام مواصفات خاصّة به، فمثلا؛ فإنّ مواصفات مراكز البيانات تحدّد الأجهزة التي يمكن استخدامها في حالة رغبة المستخدم في القضاء على الأعطال التّي من شأنها التّسبب في توقف المعالجة في الخادمات.

8– 9– إدارة الامتثال والتّوافق: Compliance management تعني هذه المواصفة هنّا بالتأّكد من أنّ المؤسسة مطبقة وملتزمة بجميع المتطلّبات والتّشريعات القانونيّة، والتّشريعيّة المتعلقة بأمن البيانات والمعلومات الرقميّة والمعمول بها داخل الجماهير العظمى، وبذلك تضمن عدم الوقوع في مخالفات قانونيّة للتّشريعات النّافذة، أو أن تتّم عمليّات اختراق أمنيّة من خلال تطبيق إجراءات غير رسميّة، كما تشمل الالتزام بالسياسات التّي وضعتها المؤسسة في مجال أمن البيانات وإجراءات المراجعة الداخليّة.

9– فوائد الحصول على شهادة الآيزو ISO27001

– من أهم فوائد الشهادة هي وضع معالم نظام أمن المعلومات في المنظمة وبناء نظام متكامل يعتمد على عمليّات مستمرة يؤدي تطبيقها على الحماية المرجوة والتطور المستمر بناء على منهجيّة معتمدة؛

– مؤشر بالتزام المنظمة على جميع مستوياتها بحماية المعلومات؛

– زيادة الثّقة بالمنظمة ونقطة تنافسيّة مهمّة.

الخاتمة: تتمثّل أهم النتائج التّي توصلت إليها في ما يلي:

– الحفاظ على المعلومات من المسائل المهمّة في الحياة؛

– خطر الكشف على المعلومات الخاصّة؛

– ضرورة أخذ الحيطة والحذر لتحقيق سلامة المعلومات

– أهميّة المعلومات بالنسبة للفرد والمجتمع؛

– تعدد طرق تخريب المعلومات؛

– بروز جهود منظمة العالمية للتقييس في الحفاظ على سلامة وشرية المعلومات؛

– أهمية التخطيط في العناية بالمعلومات؛

– ترجمة وتوضيح الأمن كما تم تعريفه في القواعد والمبادئ والأهداف العليا للمنظمة؛

– بيان الإجراءات التّي يجب إتباعها لتفادي المخاطر والمهددات والتّعامل معها إذا ما وقعت السّرقة والاعتداءات.

قائمة المراجع:

---

1 ـــ معنى المنظمة العالمية للمواصفات القياسية الآيزو في معجم المعاني الجامع عن الموقع الإلكتروني:www. Almany. Com/ar/dict/ar_ar/

2 ـــ معنى المنظمة العالمية للمواصفات القياسية الآيزو في معجم المعاني الجامع عن الموقع الإلكتروني: .www. Almany. Com/ar/dict/ar_ar/

3 ـــ منصف ملوك، أثر إشهاد الجودة على أداء المؤسسات الجزائرية حالة المواصفة Iso9001 دراسة إحصائية بالمؤسسة الوطنية لأجهزة القياس والمراقبة، مذكرة لنيل شهادة الماجستير، جامعة فرحات عباس، سطيف: 2010، ص45.

4 ـــ المرجع نفسه، ص49.

5 ـــ ينظر: المرجع نفسه.

6 ـــ سوسن شاكر مجيد، محمد عواد الزيادات، إدارة الجودة الشاملة وتطبيقاتها في الصناعة والتعليم، ط1. عمان: 2007، دار الصفاء للنشر والتوزيع، ص139.

7 ـــ عن الأيزو 27001 "حماية وسرية المعلومات" عن الموقع الإلكتروني: www.google.dz

8 ـــ الأمن المعلوماتي لأنظمة المعلومات: عن الموقع الإلكتروني: www.google.dz

9 ـــ ينظر: منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها، مذكرة لنيل شهادة الماجستير، جامعة نايف للعلوم الأمنية: 2008.

10 ـــ ينظر: المرجع نفسه.

11 ـــ ينظر: منصور بن سعيد القحطاني: مهددات الأمن المعلوماتي وسبل مواجهتها، مذكرة لنيل شهادة الماجستير جامعة نايف للعلوم الأمنية: 2008.

12 ـــ عثمان أبو بكر القاجيجي،" تطبيق المواصفة الليبيبة 27001 لأمن وسرية البيانات الرقمية في مراكز نظم المعلومات الجغرافية بالجماهير العظمى"، عن الموقع الالكتروني:www. Google. dz

13 ـــ ينظر: المرجع نفسه.

14 ـــ ينظر المرجع نفسه.

15 ـــ عثمان أبو بكر القاجيجي، "تطبيق المواصفة الليبيبة 27001 لأمن وسرية البيانات الرقمية في مراكز نظم المعلومات الجغرافية بالجماهير العظمى"، عن الموقع الالكتروني: www.google.com